

Security Challenges in Communication Networks

Authentication in Constrained Settings

Katerina Mitrokotsa

11th of April 2013,
Universiteit van Amsterdam
Amsterdam, The Netherlands



Short Bio

- **PhD** Department of Informatics University of Piraeus, Greece



Title: **“Intrusion Detection in Computer Networks Using Machine Learning Algorithms”**.

- Visitor Assistant Professor, Department of Computer Science,



Vrije Universiteit, Amsterdam, The Netherlands

- Postdoctoral Researcher in Faculty of EEMCS, **Delft University of Technology**,



- Marie Curie Fellow - Senior Researcher in LASEC, EPFL



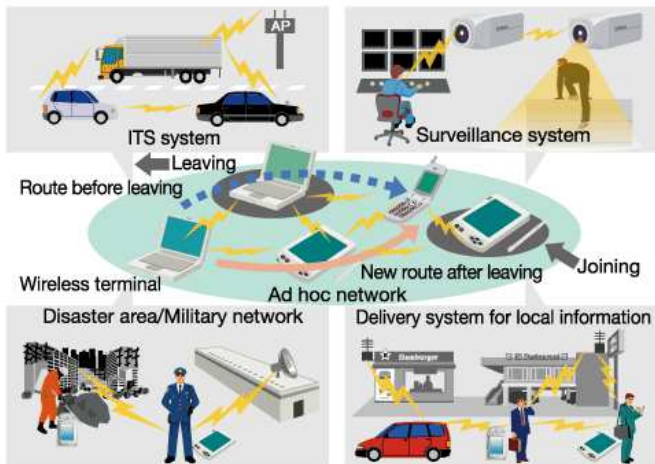
- Professor University of Applied Sciences Western Switzerland (HES-SO)



Outline

- Wireless communications
- Security & privacy risks in communications
- How can we achieve security?
- Highlights of my current-previous research
- Future work
- Conclusions

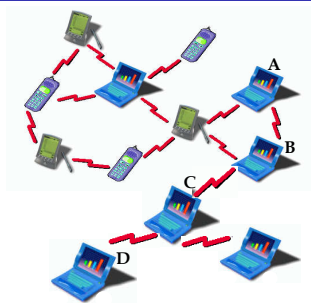
Applications of Wireless Communications



Wireless Communications

ad hoc networks

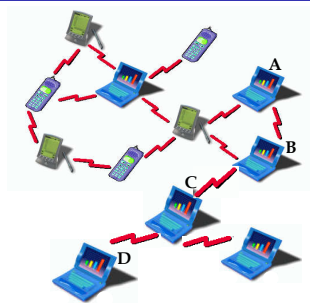
- A network of nodes connected by **wireless** links.
- Communication through **neighbours**.
- **Pros:** Easy & quick deployment
- **Cons:** open medium, power constraints, no centralised infrastructure.



Wireless Communications

ad hoc networks

- A network of nodes connected by **wireless** links.
- Communication through **neighbours**.
- **Pros:** Easy & quick deployment
- **Cons:** open medium, power constraints, no centralised infrastructure.



RFID systems

Radio Frequency Identification

- **RFID Tags:** integrated circuits equipped with antennas.
- **RFID Readers:** radio communication with RFID tags.
- **Back-end-Databases:** collect information related to tagged objects.



Applications of RFID Systems

Possible Applications

- Public Transportation.
- e-passports (since 2004).
- Controlling Building Access (i.e. military bases, airports).
- Automobile Keys.
- Animal Tracking.
- Improve Inpatient safety.



Aspects of Security

Security Primitives

- **Availability:** Assurance that information systems & services are **accessible**.
- **Confidentiality:** Ensures that information is **never** disclosed to unauthorized parties.
- **Integrity:** Information **can not** be modified without detecting it.
- **Authentication:** A party is able to ensure the **identity** of the party it is communicating with.
- **Non-repudiation:** Ensures that the origin of a message **can not deny** having sent the message.

Security Risks

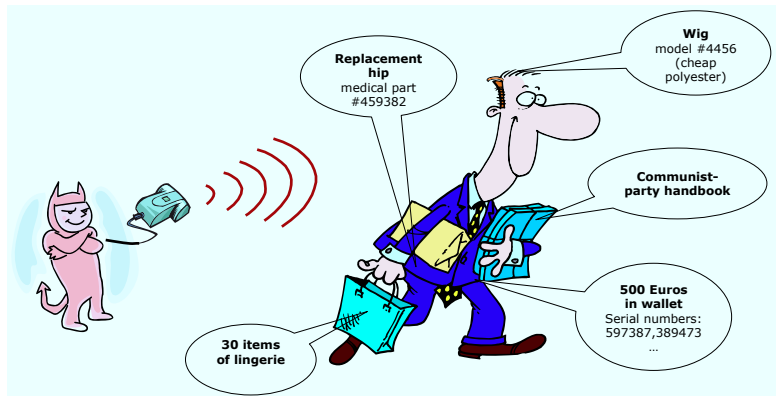
What is an Intrusion?

- Any set of actions that attempt to **compromise** the **integrity**, **confidentiality** or **availability** of a resource.

Common Attacks

- Impersonation attacks: i.e. cloning
- Information leakage/modification
- Denial of Service attacks: flooding, selfish behaviour
- Relay attacks
- ...

Security Risks - Privacy Issues



Privacy Violation

- Retrieve **sensitive** data.
- Profiling users.
- Tracking.

How to Achieve Security?

Intrusion Prevention

- **First line** of defense.
- Safeguard systems against attacks. Stop attacks from being launched.
- Employ authentication protocols, encryption algorithms.
- Reduce intrusions but **not eliminate** them.

How to Achieve Security?

Intrusion Prevention

- **First line** of defense.
- Safeguard systems against attacks. Stop attacks from being launched.
- Employ authentication protocols, encryption algorithms.
- Reduce intrusions but **not eliminate** them.

Intrusion Detection

- A **second wall** of defense.
- Mechanisms to detect an attack, preferably at an **early stage**.

How to Achieve Security?

Intrusion Prevention

- **First line** of defense.
- Safeguard systems against attacks. Stop attacks from being launched.
- Employ authentication protocols, encryption algorithms.
- Reduce intrusions but **not eliminate** them.

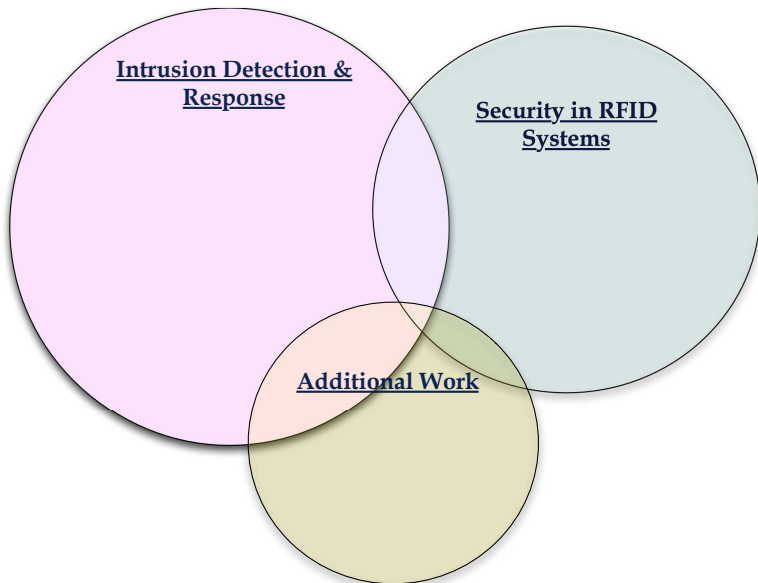
Intrusion Detection

- A **second wall** of defense.
- Mechanisms to detect an attack, preferably at an **early stage**.

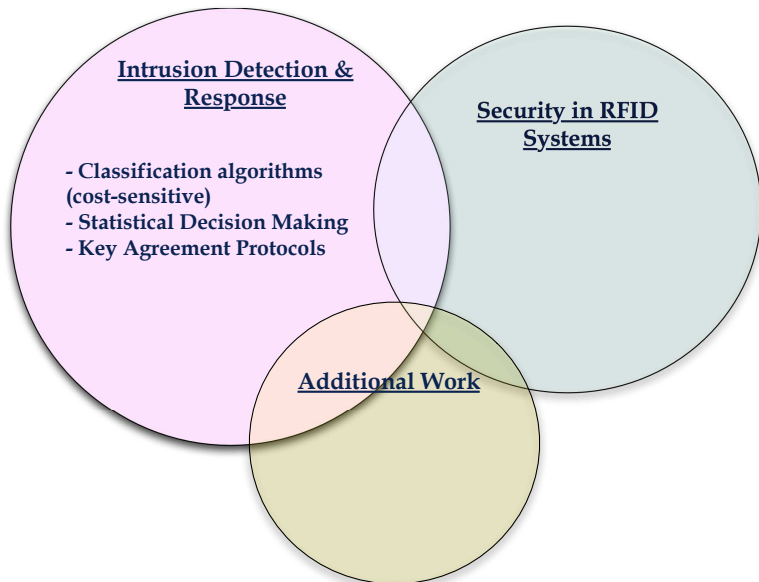
Intrusion Response

- Respond in order to mitigate the **impact** of the attack.

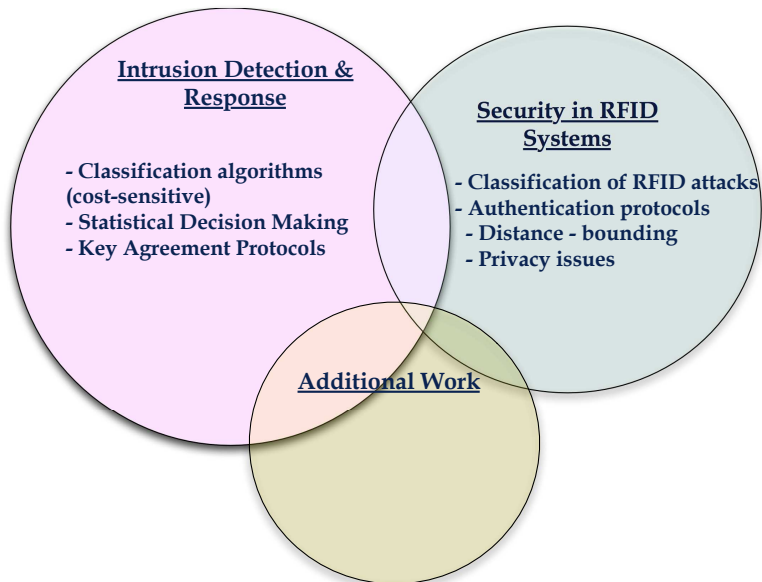
My Research



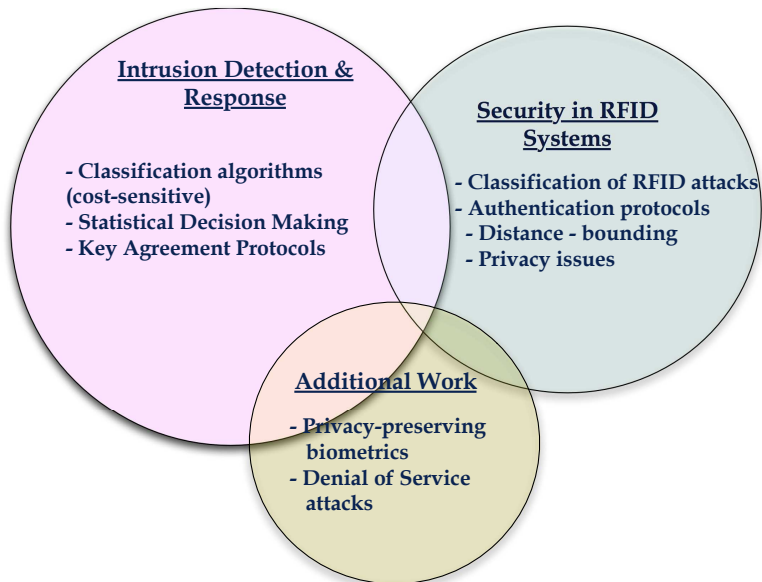
My Research



My Research



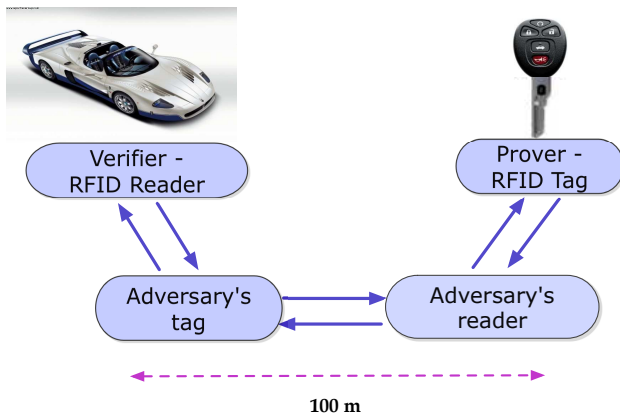
My Research



RFID Security

Relay attack

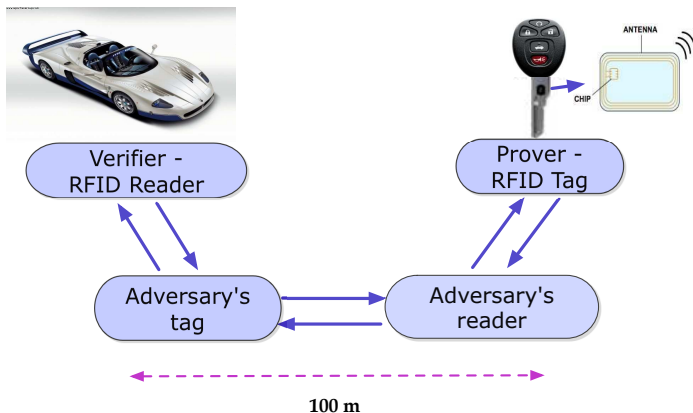
- Communication **Range**: a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



RFID Security

Relay attack

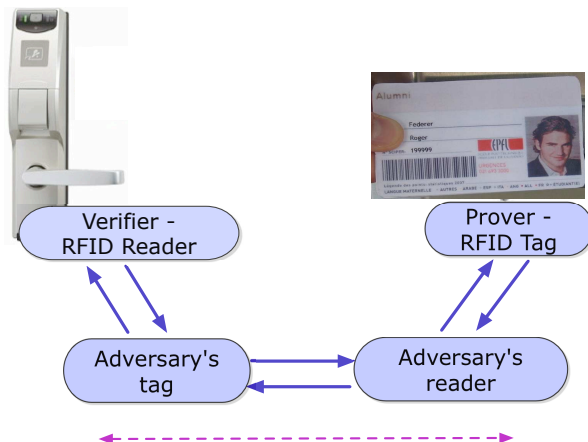
- Communication **Range**: a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



RFID Security

Relay attack

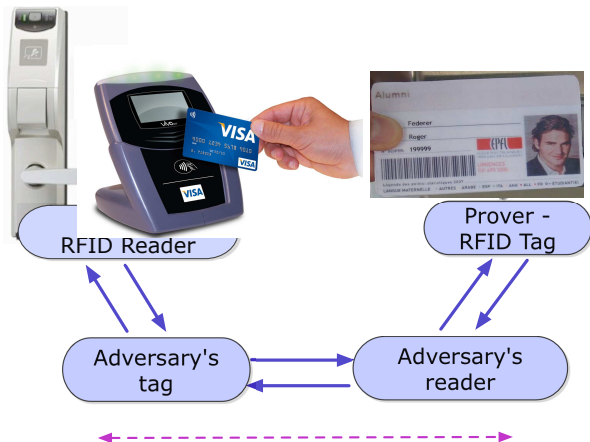
- Communication **Range**: a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



RFID Security

Relay attack

- **Communication Range:** a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



RFID Security

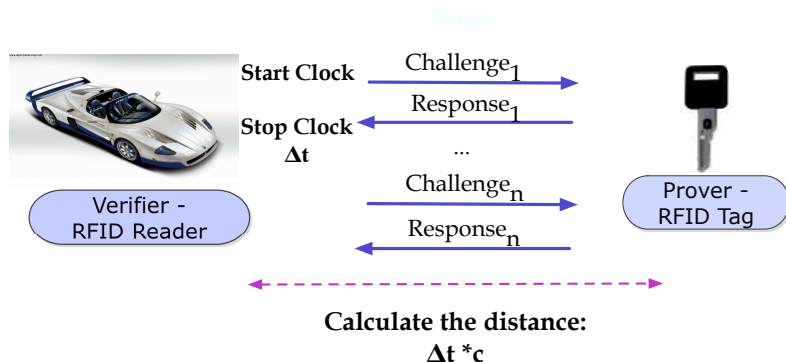
Relay attack

- Communication **Range**: a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



RFID Security

Countermeasure against relay attacks: **Distance-Bounding** protocols

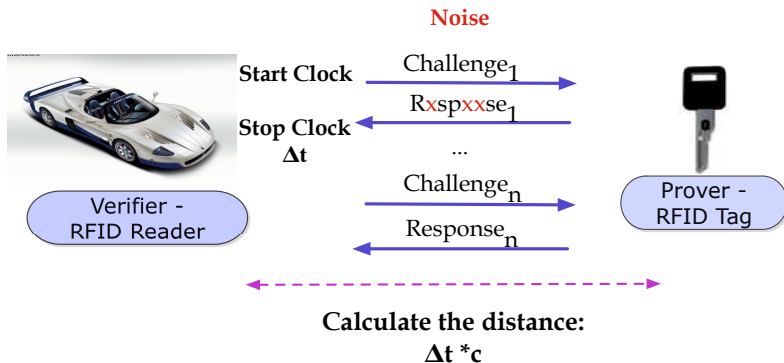


RFID Security

Distance-Bounding protocols: Goals

- Minimise the **resource cost**
- Maximise/Minimise the probability of authenticating a **legitimate user/attacker**.

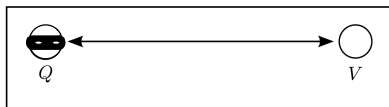
Problem: **noise** increases the probability of error.



Relay Attacks & DB

a) Distance Fraud

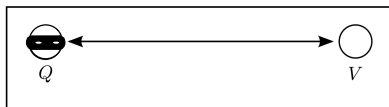
[Brand & Chaum, EUROCRYPT 1993]



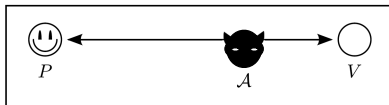
Relay Attacks & DB

a) Distance Fraud

[Brand & Chaum, EUROCRYPT 1993]



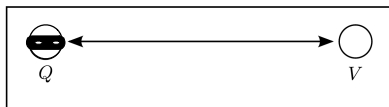
b) Mafia Fraud [Desmedt SECURICOM 1988]



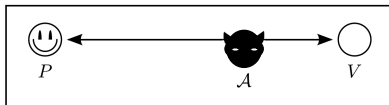
Relay Attacks & DB

a) Distance Fraud

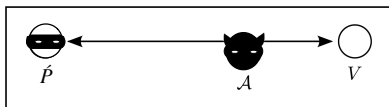
[Brand & Chaum, EUROCRYPT 1993]



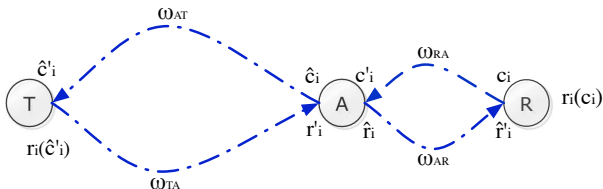
b) Mafia Fraud [Desmedt SECURICOM 1988]



c) Terrorist Fraud [Desmedt SECURICOM 1988]



Distance Bounding Protocols: Mafia Fraud attack



Notation:

A: attacker, R: reader, T : Tag.

$c \rightarrow$ **challenge**, $r \rightarrow$ **response**.

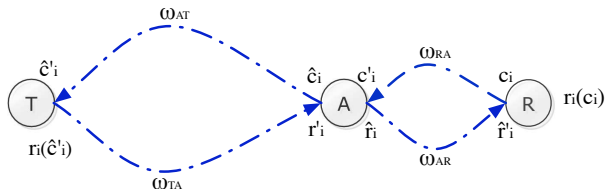
x : a message **transmitted** $\rightarrow x'$ is the message **received** (due to errors, noise).

\hat{x} : attacker's **guesses** for possible values of message x (challenge or response).

ω_{BC} : **noise** between the transmission channel of B and C.

A. Mitrokovtsa et al. "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels". *IEEE Communications Letters*, Feb. 2010.

Distance Bounding Protocols: Mafia Fraud attack



A similar **attack** has been launched against the **Dutch transport system** (OV-chipkaart) in 2008.

Notation:

A: attacker, R: reader, T : Tag.

$c \rightarrow$ **challenge**, $r \rightarrow$ **response**.

x : a message **transmitted** $\rightarrow x'$ is the message **received** (due to errors, noise).

\hat{x} : attacker's **guesses** for possible values of message x (challenge or response).

ω_{BC} : **noise** between the transmission channel of B and C.

A. Mitrokotsa et al. "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels". *IEEE Communications Letters*, Feb. 2010.

Distance-bounding protocols: Contributions

Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- Described attacks that can be launched against [Bay, Boureau, Mitrokotsa, Spulber, Vaudenay, INSCRYPT2012] [Boureau, Mitrokotsa, Vaudenay, LATINCRYPT 2012]
- Proposed new protocols that do not suffer of identified vulnerabilities [Boureau, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureau, Mitrokotsa, Vaudenay, Lightsec 2013].

Distance-bounding protocols: Contributions

Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- Proposed new protocols that do not suffer of identified vulnerabilities [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureanu, Mitrokotsa, Vaudenay, Lightsec 2013].

Distance-bounding protocols: Contributions

Contributions

- **Analysed the [security](#) of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- **Proposed new protocols that do not suffer of identified vulnerabilities** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureanu, Mitrokotsa, Vaudenay, Lightsec 2013].

Distance-bounding protocols: Contributions

Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- **Proposed new protocols that do not suffer of identified vulnerabilities** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- **Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013]

Distance bounding protocols: Contributions

- A simple (dictionary) attack successful against 4 protocols
- Leads to the full recovery of the key.
- Depends of the **length** of the nonces (random values) used to hide relationships between repeated authentication attempts.
- **Nonce repetition:** Compromise security.
- Martingale analysis of the **birthday paradox**.

Theorem

For some $q \in [0, 1]$, when $d \in \mathbb{N}$ is the number of possible nonces, we can recover a key of length k , with probability at least $1 - \delta$, $\forall \delta \in [0, 1]$ after at most t sessions:

$$t = O\left(\max\left\{\sqrt{d \ln(k)}, d^{2/3}\right\}\right) \quad (1)$$

Distance bounding protocols

Problem

- The **noise** necessitates the use of a **tolerance threshold** τ
- How do you choose the **threshold**?
- How do you choose the **number of rounds**?
- We propose an **expected loss** framework for characterising and deriving optimal solutions

[Dimitrakakis, Mitrokotsa, Vaudenay, INFOCOM'12]

Distance bounding protocols

Problem

- The **noise** necessitates the use of a **tolerance threshold** τ
- How do you choose the **threshold**?
- How do you choose the **number of rounds**?
- We propose an **expected loss** framework for characterising and deriving optimal solutions

Similar problem with CAPTCHA authentication.

[Dimitrakakis, Mitrokotsa, Vaudenay, INFOCOM'12]

Additive-error challenge-response authentication protocol

Definition

- 1 Select the number of challenge-response **rounds** n .
- 2 Select a **threshold** τ .
- 3 At the i -th round:
 - (i) The verifier sends a **challenge** c_i .
 - (ii) The prover **responds** with r_i .
 - (iii) The verifier calculates an **error** $\varepsilon_i \in [0, 1]$.
- 4 The verifier calculates the error function

$$\varepsilon \triangleq \sum_{i=1}^n \varepsilon_i$$

- 5 The verifier \mathcal{V} **rejects** the prover (authenticator) \mathcal{P} , if and only if $\varepsilon \geq \tau$.

Expected Loss Analysis

Loss

- ℓ_A : **loss** if we **authenticate** a **malicious party** A (*attacker*).
- ℓ_U : **loss** if we **fail to authenticate** a **valid party** U (*user*).
- ℓ_B : **cost** of **each round** of the challenge-response phase.

Theorem (Upper bound on expected loss)

Assume $\ell_A, \ell_U, \ell_B > 0$. If we choose $\tau = \hat{\tau}_n^*$ and

$$\hat{n}^* \triangleq \frac{\sqrt{1 + 2CK} - 1}{C},$$

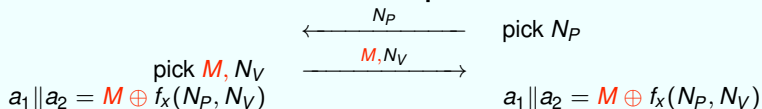
where $C = \Delta^2$ and $K = \sqrt{\ell_A \ell_U} / \ell_B$, then the expected loss $\mathbb{E} L$ is bounded as:

$$\mathbb{E}(L \mid \hat{\tau}_n^*, \hat{n}^*) \leq \frac{1}{\Delta} \sqrt{8\ell_B (\ell_A \ell_U)}^{1/4}$$

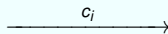
► Comparison of losses

C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, Expected loss analysis analysis of thresholded authentication protocols in noisy conditions, INFOCOM 2012

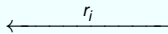
Distance-Bounding Protocols : The SKI protocol

Verifiersecret: x **Prover**secret: x **initialization phase****distance bounding phase**for $i = 1$ to n pick $c_i \in \{1, 2, 3\}$

start clock



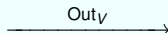
stop clock



$$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$$

check τ responses

check timers



Distance-Bounding Protocols: The SKI protocol

Circular keying

- We require that leaking $f_x(y)$, or $f_x(y) \oplus x$ or a mixture of both do not compromise security.
- An adversary \mathcal{A} making queries of the form (y_i, a_i, b_i) to an oracle:

$$y, a, b \rightarrow (a \cdot x') + (b \cdot f_{x(y)})$$

cannot distinguish if $x = x'$ or x and x' are independent.

Theorem

If f is a circular-keying secure PRF and V requires at least τ correct responses:

- All DISTANCE-FRAUDS have a success probability bounded by $\mathbb{P}[\text{success}] \geq B(b, \tau, \frac{3}{4})$
- All MIM attacks have a success probability bounded by $\mathbb{P}[\text{success}] \geq B(b, \tau, \frac{2}{3})$
- For all COLLUSION FRAUDS such that $\mathbb{P}[\text{CF succeeds}] \geq B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})^{1-c}$ there is an associated MIM with P^* such that:

$$\mathbb{P}[\text{MIM SUCCEEDS}] \geq \left(1 - B\left(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3}\right)^c\right)^n$$

$$B(n, \tau, \rho) = \sum_{i=\tau}^n \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

Distance-Bounding Protocols: The SKI protocol

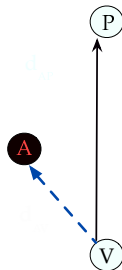
Summary regarding DB

- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- **SKI** [Serge - Katerina - Ioana] offers provable security

Information Leakage in DB Protocols

Information Leakage

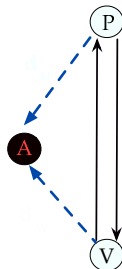
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



Information Leakage in DB Protocols

Information Leakage

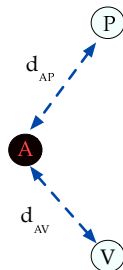
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



Information Leakage in DB Protocols

Information Leakage

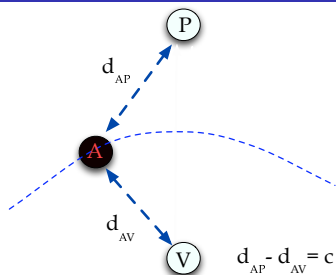
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



Information Leakage in DB Protocols

Information Leakage

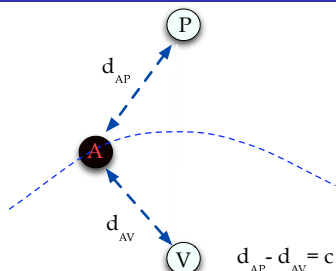
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



Information Leakage in DB Protocols

Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



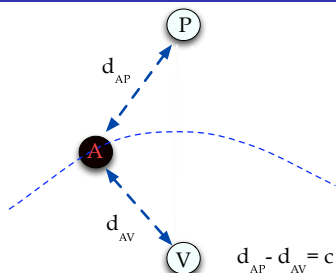
Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol [Rasmussen- Čapkun CCS 2008]
- We showed that their protocol is **susceptible** to multiple attacks.[Aumasson, Mitrokotsa, Peris-Lopez, ICICS 2011], [Mitrokotsa, Onete, Vaudenay, IEEE RFID-TA 2012]
- We proved: for limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.[Mitrokotsa, Onete, Vaudenay, Submitted]
- Proposed a new privacy-preserving DB protocol.

Information Leakage in DB Protocols

Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



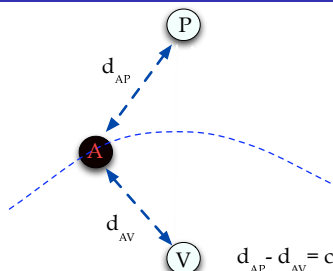
Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol [Rasmussen- Čapkun CCS 2008]
- We showed that their protocol is **susceptible** to multiple attacks. [Aumasson, Mitrokotsa, Peris-Lopez, ICICS 2011], [Mitrokotsa, Onete, Vaudenay, IEEE RFID-TA 2012]
- We proved: for limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy. [Mitrokotsa, Onete, Vaudenay, Submitted]
- Proposed a new privacy-preserving DB protocol.

Information Leakage in DB Protocols

Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



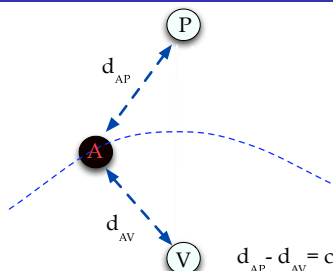
Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol [Rasmussen- Čapkun CCS 2008]
- We showed that their protocol is **susceptible** to multiple attacks. [Aumasson, Mitrokotsa, Peris-Lopez, ICICS 2011], [Mitrokotsa, Onete, Vaudenay, IEEE RFID-TA 2012]
- We proved: for limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy. [Mitrokotsa, Onete, Vaudenay, Submitted]
- Proposed a new privacy-preserving DB protocol.

Information Leakage in DB Protocols

Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



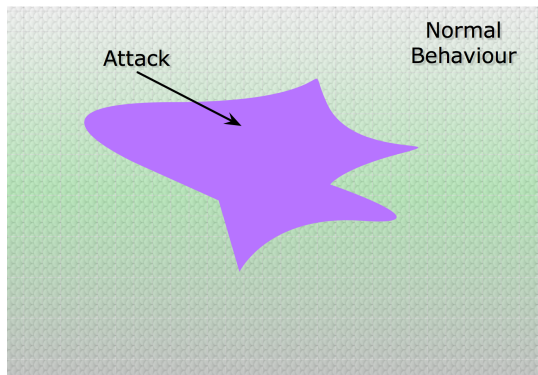
Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol [Rasmussen- Čapkun CCS 2008]
- We showed that their protocol is **susceptible** to multiple attacks. [Aumasson, Mitrokotsa, Peris-Lopez, ICICS 2011], [Mitrokotsa, Onete, Vaudenay, IEEE RFID-TA 2012]
- We proved: for limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy. [Mitrokotsa, Onete, Vaudenay, Submitted]
- Proposed a new privacy-preserving DB protocol.

Challenges for Effective Intrusion Detection

Challenges:

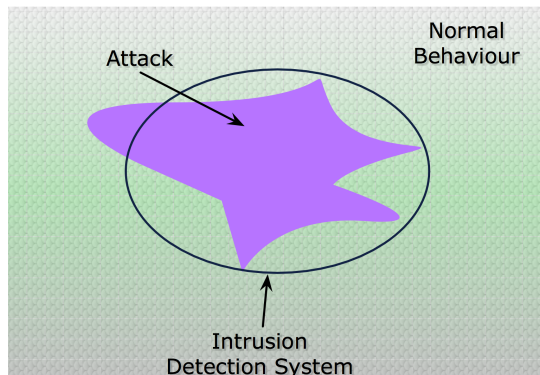
- **Detect** an attack at an early stage → **Respond** accordingly.
- Efficient **trade-off** between accurate & quick intrusion detection.



Challenges for Effective Intrusion Detection

Challenges:

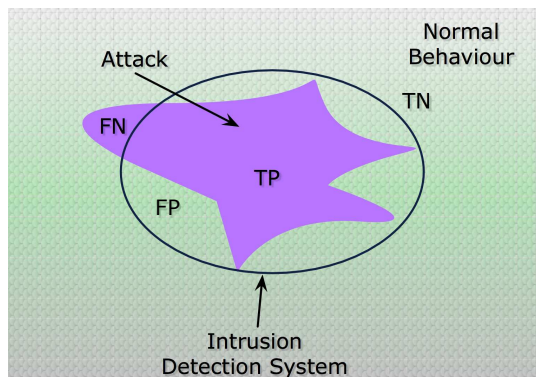
- **Detect** an attack at an early stage → **Respond** accordingly.
- Efficient **trade-off** between accurate & quick intrusion detection.



Challenges for Effective Intrusion Detection

Challenges:

- **Detect** an attack at an early stage → **Respond** accordingly.
- Efficient **trade-off** between accurate & quick intrusion detection.



TP: True Positive

TN: True Negative

FP: False Positive

FN: False Negative

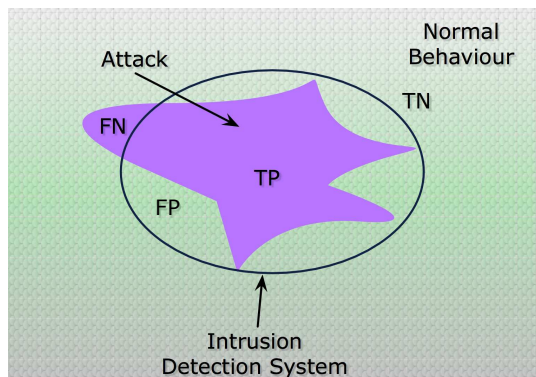
Challenges for Effective Intrusion Detection

Challenges:

- **Detect** an attack at an early stage → **Respond** accordingly.
- Efficient **trade-off** between accurate & quick intrusion detection.
- **Reduce** the False Alarm rate (FA) & **increase** the Detection Rate (DR).

$$DR = \frac{TP}{TP + FN},$$

$$FA = \frac{FP}{TN + FP}$$



TP: True Positive

TN: True Negative

FP: False Positive

FN: False Negative

Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

C. Dimitrakakis, A. Mitrokotsa "Near-Optimal Node Blacklisting in Adversarial Networks", GameSec 2012

Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

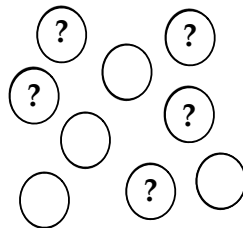
Intrusion Response: a decision making problem.

Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

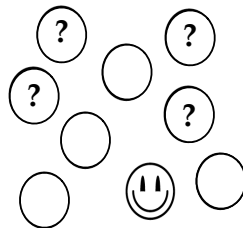


Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for **various traffic conditions**, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

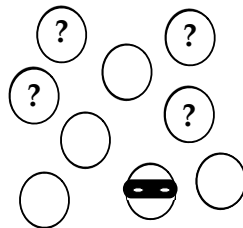


Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

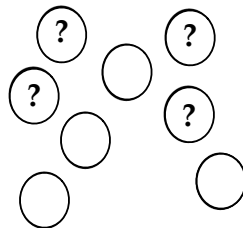


Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.



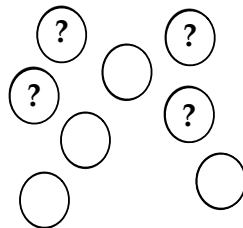
Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for **various traffic conditions**, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

Remove a node **permanently** or **keep** it for **at least one more** time step.



Intrusion Detection & Response

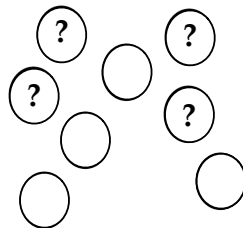
Intrusion detection & classification

- **Evaluation** for **various traffic conditions**, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

Remove a node **permanently** or **keep** it for **at least one more** time step. ↓

Goal: find a **response** strategy that **minimises** the **expected loss**.



Intrusion Detection & Response

Intrusion detection & classification

- **Evaluation** for various traffic conditions, attacks.
- Simple classification vs. cost-sensitive classification
- Hyper-parameter tuning when new unknown attacks are included in the test dataset.
- Intrusion detection & statistical decision making.

Intrusion Response: a decision making problem.

Remove a node **permanently** or **keep** it for **at least one more** time step. ↓

Goal: find a **response** strategy that **minimises** the **expected loss**.

Contributions

- Analysed empirically & experimentally a number of algorithms
- HiPER & three algorithms based on POMDPs

Intrusion detection & response

Goals

- Minimise false alarms
- Guarantee network performance.

Problems

- Adversary tries to avoid detection or manipulate the detection algorithm
- Data distribution **non** stationary

Intrusion detection & response

Goals

- Minimise false alarms
- Guarantee network performance.

Problems

- Adversary tries to avoid detection or manipulate the detection algorithm
- Data distribution **non** stationary

Methods

- Go beyond static models \Rightarrow Use **dynamic** detection models
- Extend intrusion response approaches to **colluding** nodes
- Use regret minimization algorithms
- Prediction with **limited** labels

Spam detection

- Cost of asking users to label email messages
- Cost of throwing email messages to the trash

Privacy-preserving biometrics

Problem

- Get authenticated **without revealing** information that violate our **privacy**.
- Prove possession of a valid signature for an id, without leakage of information.

Authentication vs. Identification

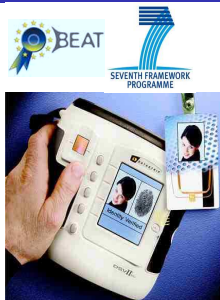


Privacy-preserving biometrics

Problem

- Get authenticated **without revealing** information that violate our **privacy**.
- Prove possession of a valid signature for an id, without leakage of information.

Authentication vs. Identification



Example

- e-passports: Cross borders without revealing **sensitive** data such as: age, nationality, facial image.
- Health: buy medication without revealing information about the diseases we have.

Tools, directions

- Use homomorphic encryption.
- Zero-knowledge proofs: authenticate data without leaking any transferable proof.

Privacy-preserving speech enhancement

DiSPEnSe: **D**istributed **S**ignal **P**rocessing **E**nhancement **S**ecurity & Privacy

Privacy & security preserving distributed signal processing speech enhancement in WSNs.

In collaboration with:

- TU Delft, Netherlands



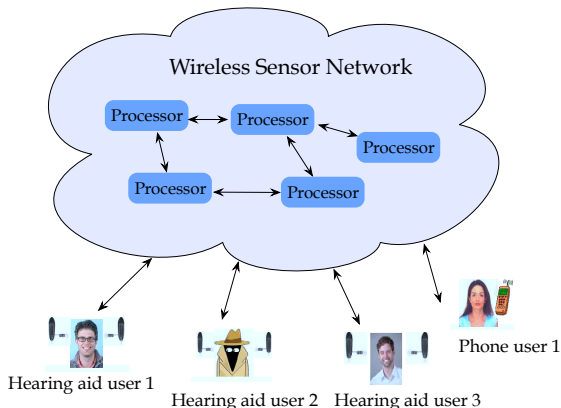
- Carl von Ossietzky Universität Oldenburg, Germany



Privacy-preserving speech enhancement

Why?

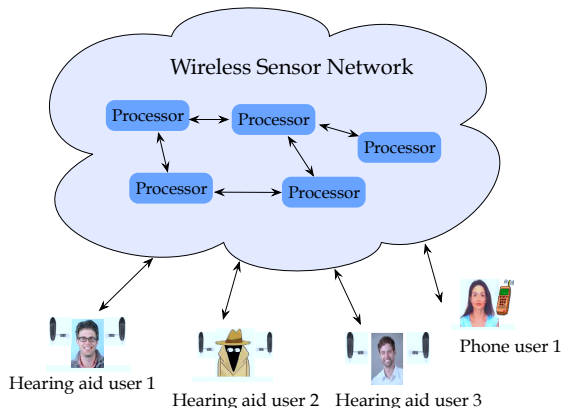
- Hearing aid users, cochlear implants, speech recognition systems ...
- **Problem:** Noise \Rightarrow quality of speech, intelligibility degraded
- Speech enhancement though WSN can have important advantages



Privacy-preserving speech enhancement

Security & Privacy guarantees

- Shared microphones & processors to **increase** speech enhancement
- Keep **private** the content of their conversation
- Eavesdropping by people outside the room **should not be possible!**



Privacy vs. cost & accuracy

Privacy vs. Computation Cost

- Given a communication network where nodes exchange data
- Some of these data are encrypted while other not
- Encrypted data \Rightarrow **Privacy** but extra cost for encryption & decryption.
- What would be my expected **loss in privacy** if I **do not encrypt** the data?

Privacy vs. cost & accuracy

Privacy vs. Computation Cost

- Given a communication network where nodes exchange data
- Some of these data are encrypted while other not
- Encrypted data \Rightarrow **Privacy** but extra cost for encryption & decryption.
- What would be my expected **loss in privacy** if I **do not encrypt** the data?

Example

- Searching in an online database information for a disease
- Giving exact description of the symptoms and name of the disease keywords
- **Privacy loss**: reveal information about the disease I may have
- **Accuracy gain**: finding out what I am looking for

Privacy vs. cost & accuracy

Privacy vs. Computation Cost

- Given a communication network where nodes exchange data
- Some of these data are encrypted while other not
- Encrypted data \Rightarrow **Privacy** but extra cost for encryption & decryption.
- What would be my expected **loss in privacy** if I **do not encrypt** the data?

Example





- Searching in an online database information for a disease
- Giving exact description of the symptoms and name of the disease keywords
- **Privacy loss**: reveal information about the disease I may have
- **Accuracy gain**: finding out what I am looking for

Trade-off accuracy vs. **Privacy**

Collaboration with groups in UvA

- Informatics Institute
 - System and Network Engineering group
 - Computational Science group
 - Intelligent Systems group
 - Federated Collaborative networks group

Funding

- Project leader of the **Rubicon**  project.
Title: **“Intrusion Detection in Ubiquitous Computing Technologies”** (55.000 €).
- Project leader of the project
“Intrusion Detection & Response in Wireless Communications”.
Funded by the **ICT talent grant**  (∼35.000 €).
- Project leader of the **Marie Curie IEF**  project
“Privacy-preserving Intrusion Detection and Response in Wireless Communications” (∼ 166.000 €).
- Partner in the **FP7 Cooperation** Project 
BEAT: Biometrics Evaluation & Testing (∼ 3.5 millions €).
9 Partners.

Professional Activities

- **Member of ENISA's Permanent Stakeholders Group (PSG):** 2012-2015
- **Member of expert groups** for ENISA ([European Network & Information Security Agency](#))
- **Member of the ERCIM WG:** Security & Trust Manament
- **Editor:**
[IEEE Communications Letters](#),
Computers & Security (Elsevier)
- **Guest editor** in special issues:
 - Journal of Networks & Computer Applications (Elsevier).
 - IEEE Transactions on Dependable & Secure Computing (IEEE).
 - Journal of Personal & Ubiquitous Computing (Springer).
- **Co-chair:** AfricaCrypt 2012, PSDML 2010, IWRT 2010, IWRT 2009.
- **Program committee:** RFIDsec 2013, IEEE CNS 2013, ARES, 2013, PST 2013, WISTP 2013, AfricaCrypt 2012, Alsec 2012, RFID EURASIP 2012, WISTP 2012, ICNS 2012...

Teaching Experience

- [Advanced Topics in Network Security](#), (Msc. Program) Department of Computer Science, Vrije Universiteit.
- [Computers & Network Security](#), (Msc. Program) Department of Computer Science, Vrije Universiteit.
- [Cryptography & Security](#), (Msc. Program) Faculty of EEMCS, TU Delft.
- [Security Protocols & Applications](#), Seminar Course, (Msc. Program) School I&C, EPFL.
- [Network Security](#) (Bsc. Program), School I&C, EPFL.
- [Information Security](#), (Bsc. Program) HES-SO.
- University of Piraeus:
 - Web Technologies.
 - Computer Networks.
 - Introduction to computing.

Network

- Delft University of Technology (TU Delft),



- Vrije Universiteit, Amsterdam



- University of Piraeus, Greece



- European Network of Information Security Agency (ENISA)



- Carl von Ossietzky Universität Oldenburg, Germany



- Carlos III University of Madrid, Spain



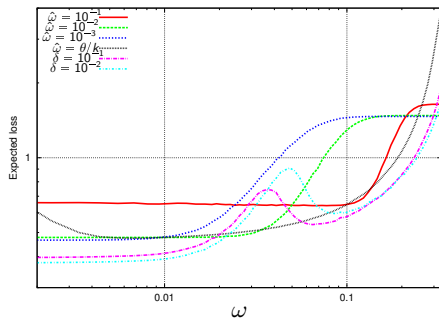
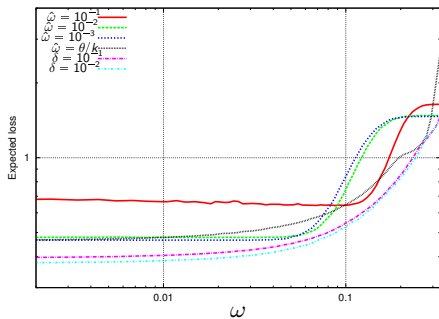
Universidad
Carlos III de Madrid

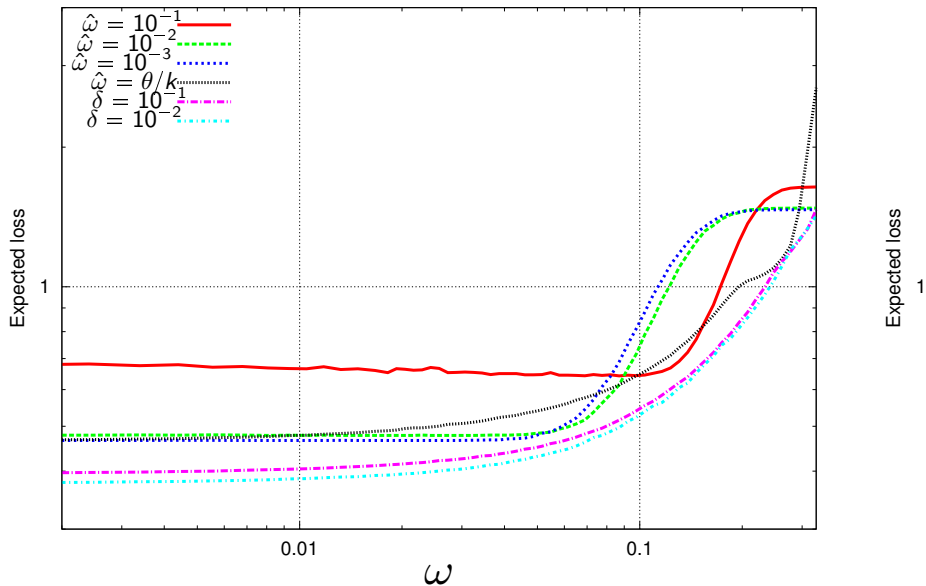
- EPFL
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

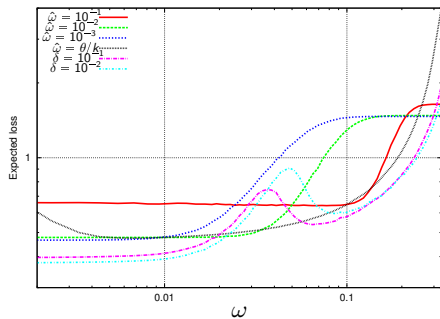
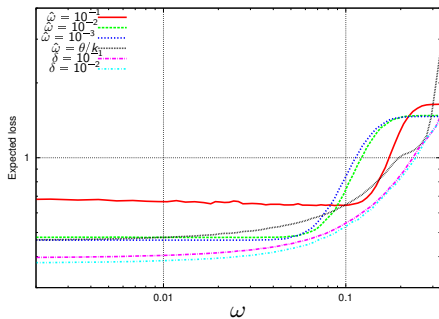


Thank you for your attention!

Comparison of losses


[► Back](#)




[► Back](#)

