Why you never, ever should roll your own security protocol

Magnus Forsell

Per-Erik Granstam

Johannes Nordh

(Yes, we are three)

Background

- Security is never any stronger than the weakest link in the chain.
- Protocol design lacks a firm mathematical base and is error prone.
- Breaking a protocol is often easier than breaking the ciphers used.
- There are LOTS of faulty protocols and implementations out there.

Goals

we actually had two

- Find flaws in protocols and implement attacks against them.
- Find out if the use of security typed languages would have prevented these flaws

What we have done

- Investigated flaws in SSL v2 and v3 and implemented some nice, workable attacks
- Investigated flaws in SSH and implemented an attack we haven't found a use for yet.
- Investigated CHAP and the mistakes Microsoft did when implementing MS-CHAP

SSL

- SSL v1?
- SSL v2 has a serious flaw, an attacker can select which cipher should be used.
- Some SSL v3 server implementations allows for an attacker to override client version and make the session be in SSL v2 instead.
- We'll show you how in a minute or two.

SSH

- SSH version 1 vs SSH version 2
- SSH suffers from the same kind of version downgrade as SSL, but in this case it even simpler.
- SSH has MITM warning messages, but doesn't consider version downgrade as an attack.
- The attack isn't as rewarding as with SSL.

This is boring, let's attack something

This is boring, let's attack something

- Start by finding a vulnerable server, hint: https://webmail.chalmers.se
- Find some unsuspecting users.
- Intercept, modify and log their traffic.

This is boring, let's attack something

- Get a LOT of computers....
- Start chewing encryption keys.
- Wait 27 hours. (don't worry we have prepared this step)
- Use the key to decrypt the login request.

This is boring, let's attack something

- Login
- Read mail
- PROFIT!

Conclusions

- Simply stay away from implementing your own security protocol.
- If you implement anything that acts as a server, don't use vulnerable languages like c.
- MEDIC really needs to update the their server.
- Security typed languages doesn't necessarily help anyone when dealing with protocols.
  And who would have the energy to do it anyway?

Questions?

Otherwise we'll go tell MEDIC about this now.