The Noise

Random Noise

- Researchers have all been listening for the ultra-skilled hackers hitting SCADA networks
- What we've been hearing about is non-targeted takeovers of trusted and protected networks (and a couple of SCADA networks)
- Utilities have spent the last few years adding firewalls, Intrusion Detection System, and all manner of other defenses. Why are we seeing a spike in random takeovers?

Hackers are changing their approach

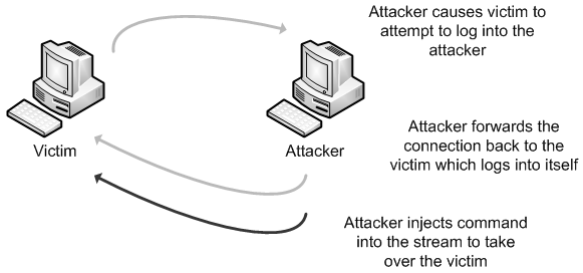
- The last five years have mostly been about three techniques
  - Buffer Overflows
  - SQL Injection
  - Cross-Site Scripting
- Those techniques have been good for attackers, but defenders have learned to auditor for those flaws
- The amount of effort required to find another buffer overflow has increased exponentially
- Hackers have had to acquire a deep knowledge of targeted protocols to find new flaws
- That deep knowledge is now being applied directly to the problems

Design Bugs

- Buffer overflows, SQL injection, and XSS are implementation problems
  - The programmer made a mistake and should fix it
- Design Bugs exist because the designer of the system or systems meant them to be there
- A series of features that are safe in and of themselves when chained together lead to a compromise

Credentials via Reflection

- Windows boxes can log into themselves
  - This is by design
- Windows networking is unencrypted
- A man-in-the-middle can be turned into a compromise



DNS Rebinding

- What www.goodguy.com doesn't always resolve the same IP address all the time
  - This is by design
- Javascript rebinding allows port scanning of the internal network
- Flash rebinding combined with reflections leads to compromise
  - It affects many other scenarios

Direct Attacks on Crypto

- Since MD5 collisions are now possible crypto systems that rely on MD5(Certificate) for authentication have been compromised
- Buffer overflows in several crypto libraries based on small intermediates are being published
  - Four guys wrote most of the popular crypto implementations and made the same mistakes everywhere
  - They're even exploitable in a .net VM
- Small totient factorization of RSA
  - Turned out not to be effective on large keys but shows the attacker community is working on the problem again

The Noise

- Off-the-shelf software is making its way onto SCADA networks
- Hackers are wielding a deep knowledge the off-the-shelf packages are developing design-level attacks
- These techniques don't give direct control of the process, but seem to be effective against the perimeter defenses being adopted by the industry

The Noise

- Will the perimeter compromises translate into high profile compromises of SCADA systems??