RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The Seven Most Dangerous New Attack Techniques and What's Coming Next

SESSION ID: EXP-T08

Moderator: Alan Paller
Director of Research
SANS Institute

Panelists:

Ed Skoudis
SANS Instructor
Counter Hack Founder

Johannes Ullrich
CTO & Dean of Research
Internet Storm Center

Mike Assante
Director
SANS Institute

Ed Skoudis

SANS Curriculum Lead for Penetration Testing

Founder of Counter Hack Challenges

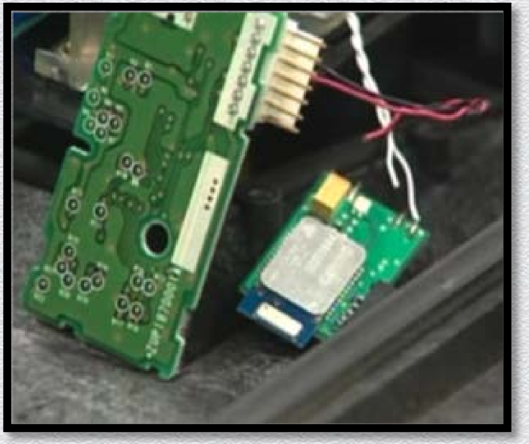
Most Dangerous New Attack Techniques

1. Bad Guys Go Wireless & Mobile
2. Air Gaps Are Dying - Innovative side channel attacks
3. Hacking the Internet of Things

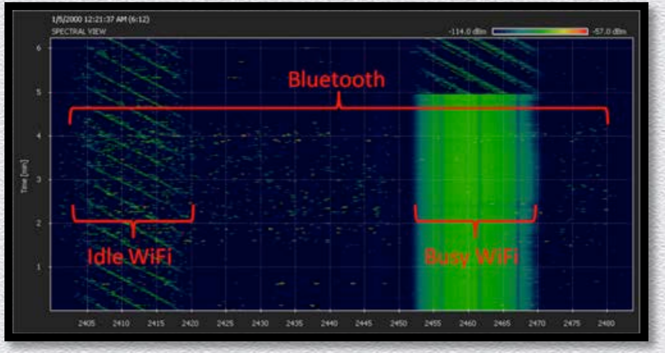
- *Trends I'm watching: Embedded systems, "Internet of Things", wireless, mobile, "There's an app for that", jail breaking, hacker culture, DIY, hobbyists, the maker movement…*

→ALL WRAPPED TOGETHER ←

Bad Guys Go Wireless & Mobile

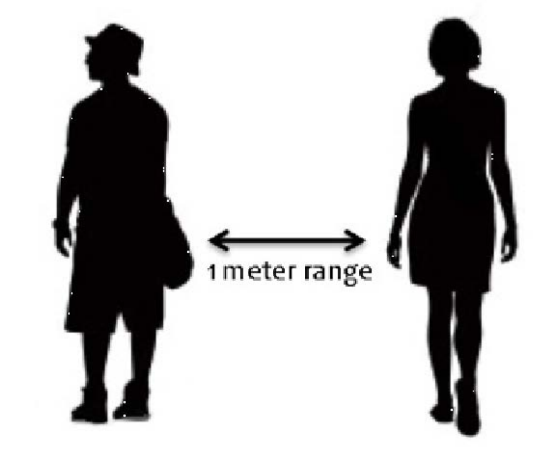


- Increasingly, we're seeing criminal attackers use wireless for their attack platforms
  - Not just as targets, but as attacker's platform
  - Untethers attackers allowing more flexibility, portability, and safety in their crimes
- In the last 12 months, we've seen a big uptick in wireless skimmers
  - Especially bluetooth, because of the dearth of tools to detect such devices
  - Freq hopping makes it hard to detect nefarious bluetooth



Using Wireless & Mobile for Attacks

- RFID skimming in hotel or retail environments for card or other ID info
- Attacks against mobile phones, tablets, and other untethered devices
- Attackers using mobile devices as attack platforms are less conspicuous

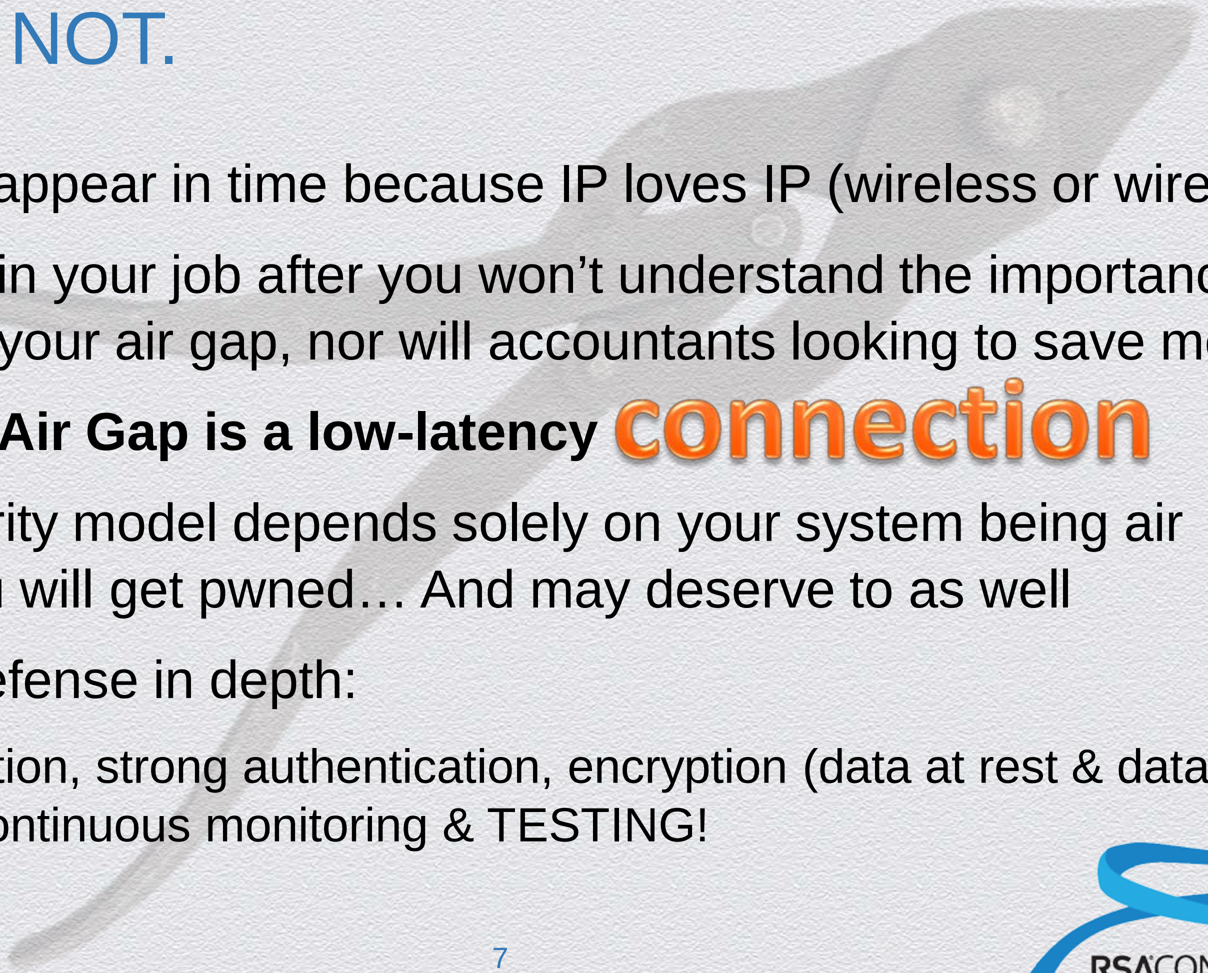


- Defenses: Turn devices off (if possible, or consider airplane mode) or shield them from attack
- If you design such devices, carefully consider replay attack vectors and DO NOT rely on the obscurity of your hardware

Air Gaps Are Dying

- Recent developments in clever side channel attacks – SOUND?!?!
  - RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis, Dec 2013
  - BadBIOS – whether real or not, the ideas are now out of the bag and widely discussed throughout Fall 2013
- And, besides these newer attacks, we face several other air-gap killers
  - USB devices carry malware (possibly including Stuxnet) across air gaps
  - Pervasive wireless (with numerous protocols) – is it really off? You sure?
  - Or, even worse, supposedly air gapped networks are interconnected to the Internet – DNS resolution, Smart Phone charging, etc.

Air Gaps? NOT.



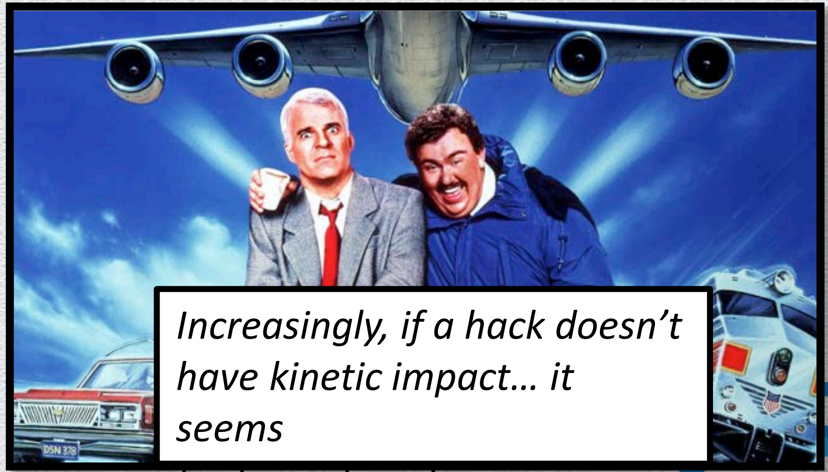
- Air gaps disappear in time because IP loves IP (wireless or wireline)
- The person in your job after you won’t understand the importance & brilliance of your air gap, nor will accountants looking to save money
- **At best, an Air Gap is a low-latency connection**
- If your security model depends solely on your system being air gapped, you will get pwned… And may deserve to as well
- Defense: Defense in depth:
  - Segmentation, strong authentication, encryption (data at rest & data in motion), continuous monitoring & TESTING!

Hacking the Internet of Things

- Our physical world is increasingly computer controlled
- Attackers are reverse engineering the underlying embedded systems
  - Stripped down OSs, typically Linux (occasionally embedded Win)
  - Usually web-based with HTTP (rarely HTTPS) & custom protocols
  - Vulns abound, but tend to be quite simple: Buffer overflows, command injection, XSS, and SQLi
- The result? Kinetic pwnage: hacking with physical impact
- In last 12 months, web cams and home router vulns
- Up next? Thermostats, electronic locks, home automation

Beyond the Small Stuff – Recent Hacker Con Talks

- HiTB Amsterdam 2013: Remotely hacking airplanes (controversy about realism and applicability, but still…)
- DEF CON 2012: Talk on hacking trains in Spain
- DEC CON 2013: Charlie Miller & Chris Valasek on hacking cars
  - Control car functions like steering & breaks via the Car Area Network
  - Additional research on wirelessly accessing car functions



Increasingly, if a hack doesn't have kinetic impact… it seems far less interesting.

Biggest Areas of Concern

- Power grid
  - The mother of all critical infrastructures
- Healthcare environments
  - Hospital systems
  - Medical devices – See Jay Radcliffe’s work
- Weapons systems
  - Disable to neutralize them
  - Turn them on their owners and operators

There are other areas of concern, such as aviation, factory automation, telecomm, etc.

Defending the Internet of Things

- Ensure you have a patching strategy for embedded systems
  - Inventory & Discovery
  - Segmentation
  - Patch process (where possible)
- Vigorously push vendors to:
  - Design security in from the start
  - Test thoroughly in advance
  - Have a rapid response strategy for discovered product vulns
  - Engage the research / hacker community proactively

Dr. Johannes Ullrich

Director and CTO of the Internet Storm Centerg

Dean of Research at SANS Technology Institute – the national graduate school for cybersecurity professionals

Bitcoin

Bitcoin

- Valuation of bitcoin is largely driven by speculation, but merchants slowly start to accept bitcoin.
- Wallet: Secret Key. Used to sign transaction
- Bitcoins are traded in public registrars, currency **is traceable but can be anonymous**
- Computers may participate in maintaining distributed transaction registers in exchange for bitcoins ("mining")
- Largely unregulated (US) or discouraged/outlawed (EU/China)

Bitcoin Theft

- A user’s private key can be stolen and used to transfer bitcoins to another user
- Secret keys are often accessible to malware
- Past Occurrences:
  - Weak random numbers used to generate keys (Android Bitcoin Wallet)
  - Malware has been used to steal keys
  - Publically displayed QR code has been stolen

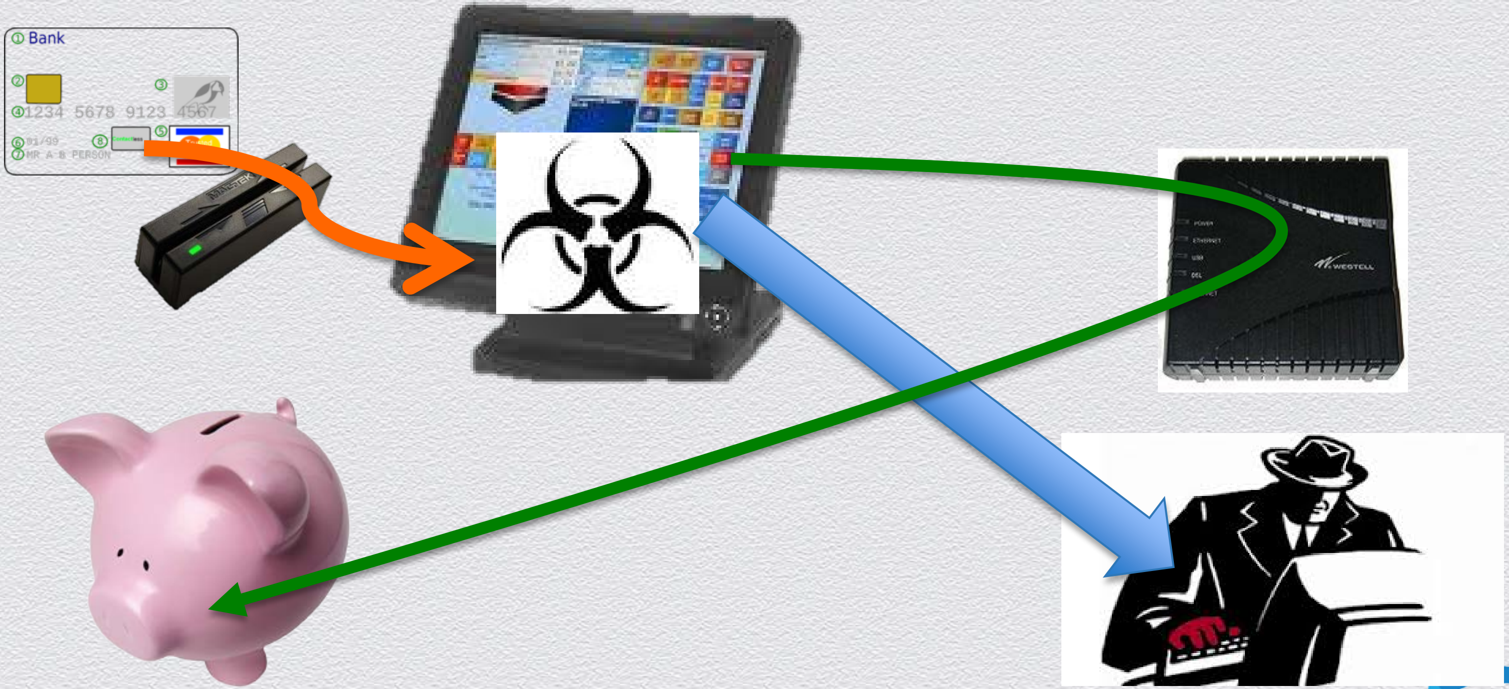
Bitcoin Mining Malware

- Simple way to monetize exploited systems
- Sometimes, bitcoin mining software is installed as an “add on” to other software
- Can go unnoticed for a long time

```
1 S www-data 13335     1 99  80   0 - 13941 -      Nov10 ?        12-
01:46:12 ./minerd -o stratum+tcp://mine.pool-x.eu:9000 -u <user> -p
<pw>--algo scrypt --no-longpoll -B
```

Point of Sale Malware

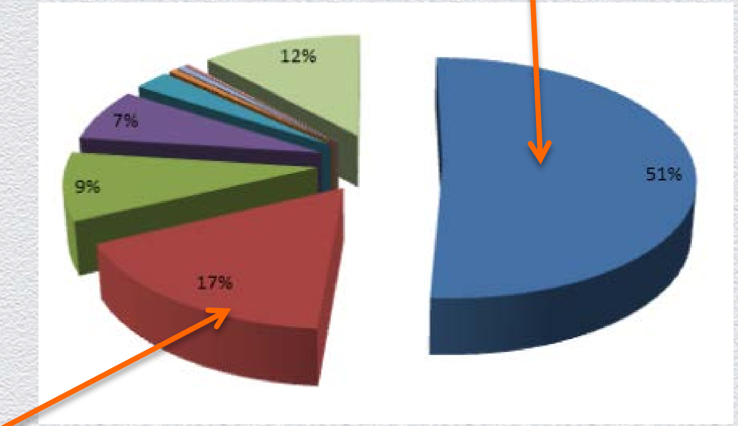
Point of Sale Malware: Data intercepted before encryption happens



Dexter/Project Hook

- Used in various attacks for over a year
- Infects Windows based PoS systems
- May be using various vulnerabilities:
  - Weak passwords
  - Drive by exploits
- Exfiltrates data in real-time

Windows XP



Windows
Home Server

Image: Seculert

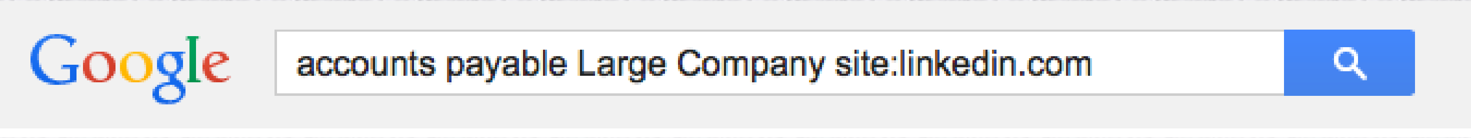
Point of Sales System Protections

- Standard “best practices” to secure systems
  - Hardened passwords
  - Firewalls
  - Patch
- Dedicated PoS systems (do not use for casual internet use)
- Encryption as close to the reader as possible

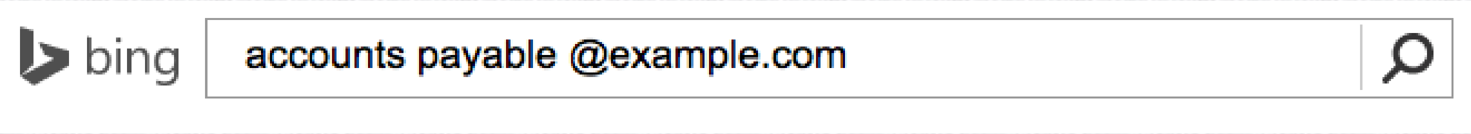
Targeted E-Mail Interception

Harvesting Social Networks

The attacker will try to identify individuals in larger corporations / banks who deal with payments (“Accounts Payable”).



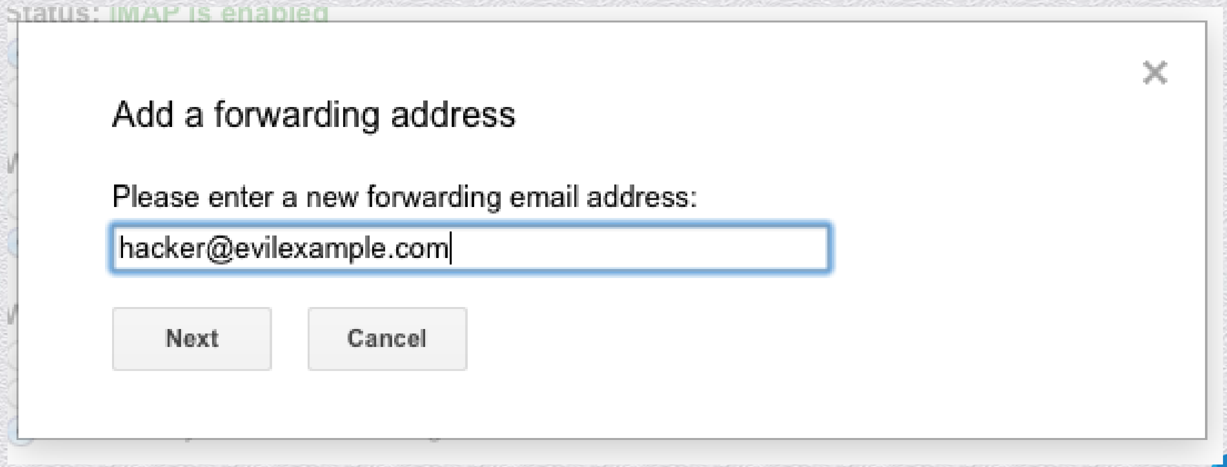
accounts payable Large Company site:linkedin.com



accounts payable @example.com

Webmail Account Takeover

- Next, the attacker will try to take control of these individual's webmail accounts (typically phishing) to add a "Forward" address to it.



Status: IMAP is enabled

Add a forwarding address

Please enter a new forwarding email address:

hacker@evilexample.com

Waiting…

- The attacker will now wait for payment related e-mail traffic.

From: Supplier

To: accounts-payable

Subject: Payment

Thanks for your payment! Can you please advise us when we can expect the next payment.

Attacker replaces/modified e-mail

- Attacker may register similar domain (if DKIM/SPF gets in the way)
- Modifies account details ("Please be advised that our payment details have changed…")
- Usually sent to the less sophisticated part of the transaction (e.g. buyer in the case of real estate, not the escrow bank)
- New account is still a US based account

Result

- Attacker will now receive payments (Large commercial transactions)
- Difficult to detect by user

  User expects e-mail. Does not suspect fraud.
- May pass manual verification by bank
- Does not require malware on user's system

Defenses

- Hardened e-mail infrastructure (e.g. two factor for webmail)
- Better e-mail authentication (Domainkeys, SPF, DMARC)
- User Awareness
- Business rules (require second person to verify account changes)

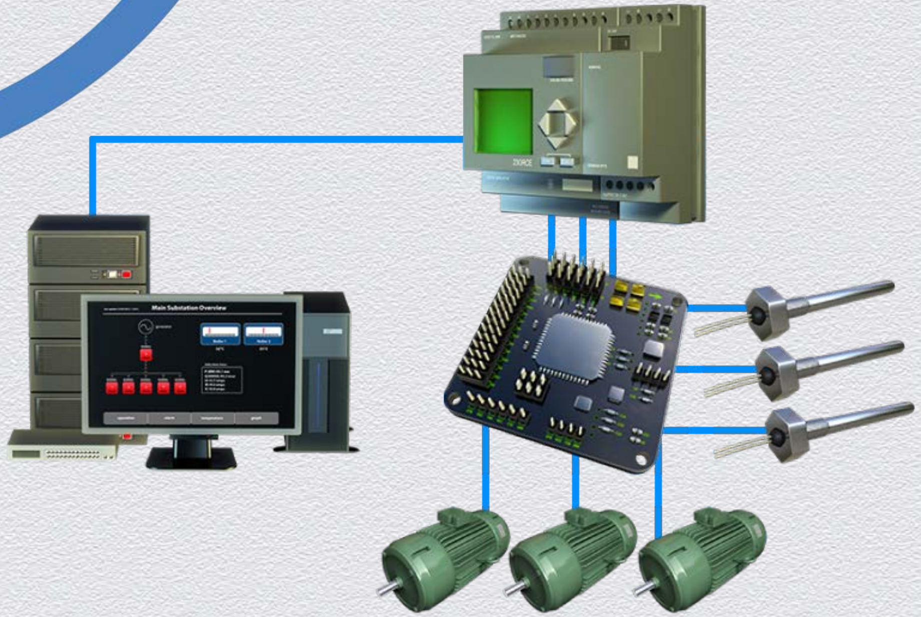
Mike Assante

Director of Industrial Control Systems programs for the SANS Institute

Previously CSO of the North American Electric Reliability Corp (NERC)

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Discovery and Compromise of Industrial Control Systems

What does it look like: Same old story?

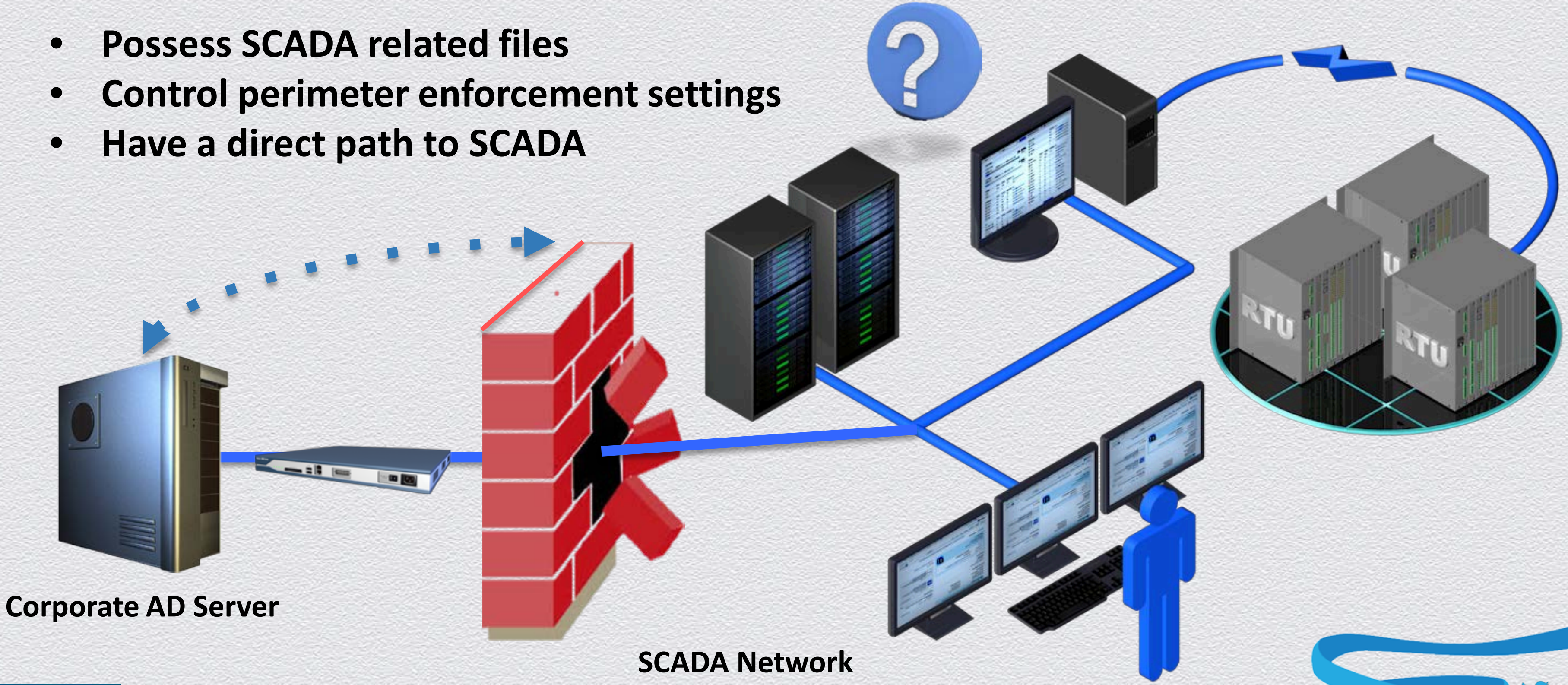
- Adversary crawls corporate page and obtains all available company personnel intel
- After performing external recon adversary targets organization with spearphishing
- Adversary establishes foothold on a small set of workstations and phones home using a reverse shell
- Adversary achieves persistence through scheduled tasks on a couple of workstations
- Performs recon (with the logged in users rights) by viewing established drive mappings, advertised network shares, and internal Directory Services
- Local credentials are stolen through cracking, pass the hash, or keyloggers

An unexpected turn: Opportunistic or planned?

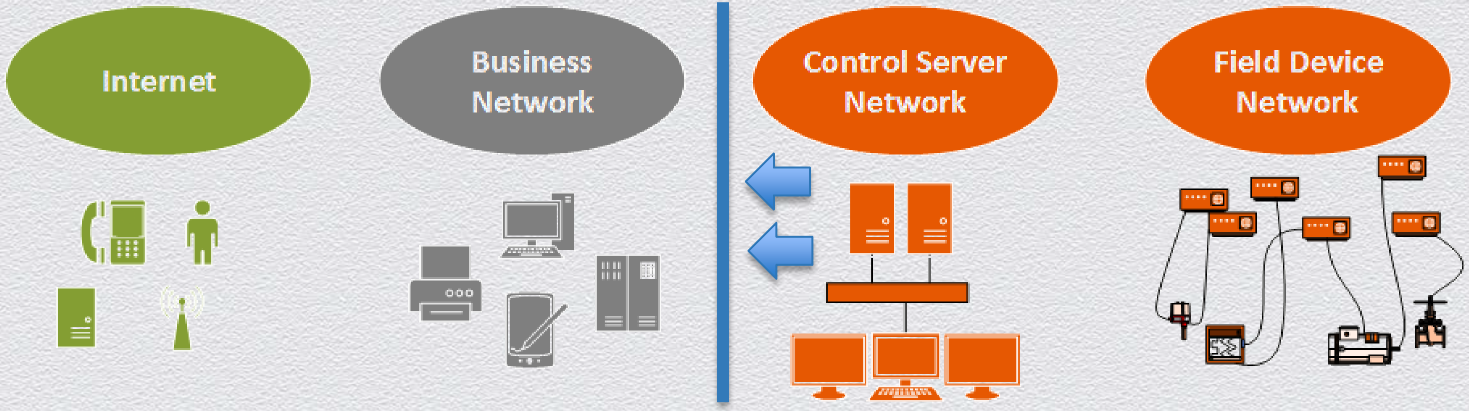
- Using appropriate credentials, they map DS by pulling down full user lists, full group listings, and full server listings
- Adversary identifies admin accounts and obtains credentials
- File systems are scavenged by looking for **specific extensions** or very **specific strings.** The data is packed up with various tools and sent out
- Adversary becomes very difficult to track, as they now potentially can be a member of any group, any user, and gain access remotely through VPN or other means
- Adversary no longer needs compromised workstations! They have become you

Keys to the Kingdom?

- Possess SCADA related files
- Control perimeter enforcement settings
- Have a direct path to SCADA

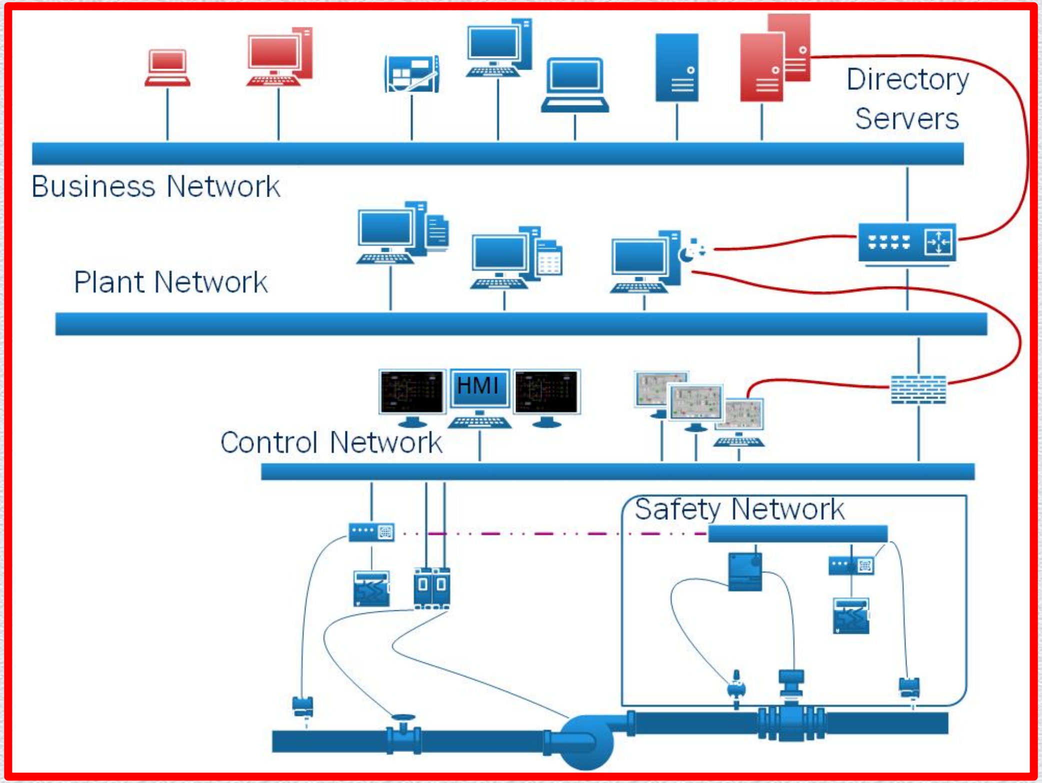


Recommended Defense: Domain Controllers in ICS



- If AD is needed in ICS, a separate domain with no relationships with business should be used
- Creation of user and workstation groups can be associated to limit access between them

High-risk architecture



Efficient use of resources = one stop shopping for mayhem

Recommended ICS Architectures (ISA-99/Purdue Model)

SANS ICS

Industrial Control Systems

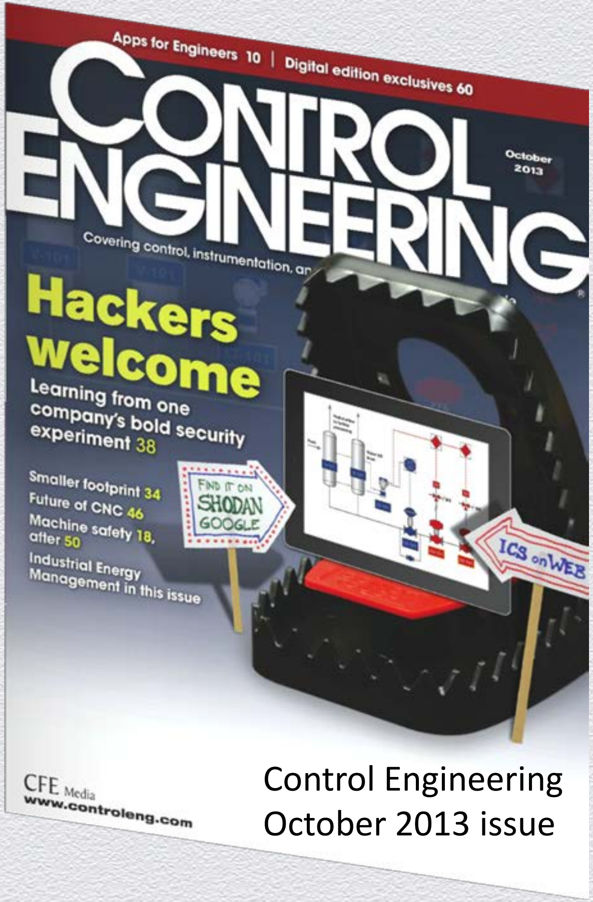
Security Resources

POSTER

FALL 2013 | 25TH EDITION

Who’s Side Are We On Anyway? – Making it too Easy

- Information Availability
- Access & Architecture
- Tools & Capability
- Politics & Reporting


Apps for Engineers 10 | Digital edition exclusives 60
CONTROL ENGINEERING
October 2013
Covering control, instrumentation, an
Hackers welcome
Learning from one company's bold security experiment 38
Smaller footprint 34
Future of CNC 46
Machine safety 18, after 50
Industrial Energy Management in this issue
FIND IT ON SHODAN GOOGLE
ICS on WEB
CFE Media
www.controleng.com

Control Engineering
October 2013 issue

Recommended Defenses (Cont.)

- Subscribe to a service that informs you of information available publicly and work to reduce it or mitigate it.
- Educate the organization on the cyber threats that exist and the responsibilities they each have
- Implement network segmentation and enforce perimeter rules in a fashion that only allows the communication needed for operation
- Examine your organizations use of Directory Services. Segment the DS environment, utilize groups to associate users to workstations, ensure alerting is enabled to notify when a user is attempting to authenticate in an abnormal manner.

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Discussion

and

What’s Coming Next?