Attacking and Defending the Grid

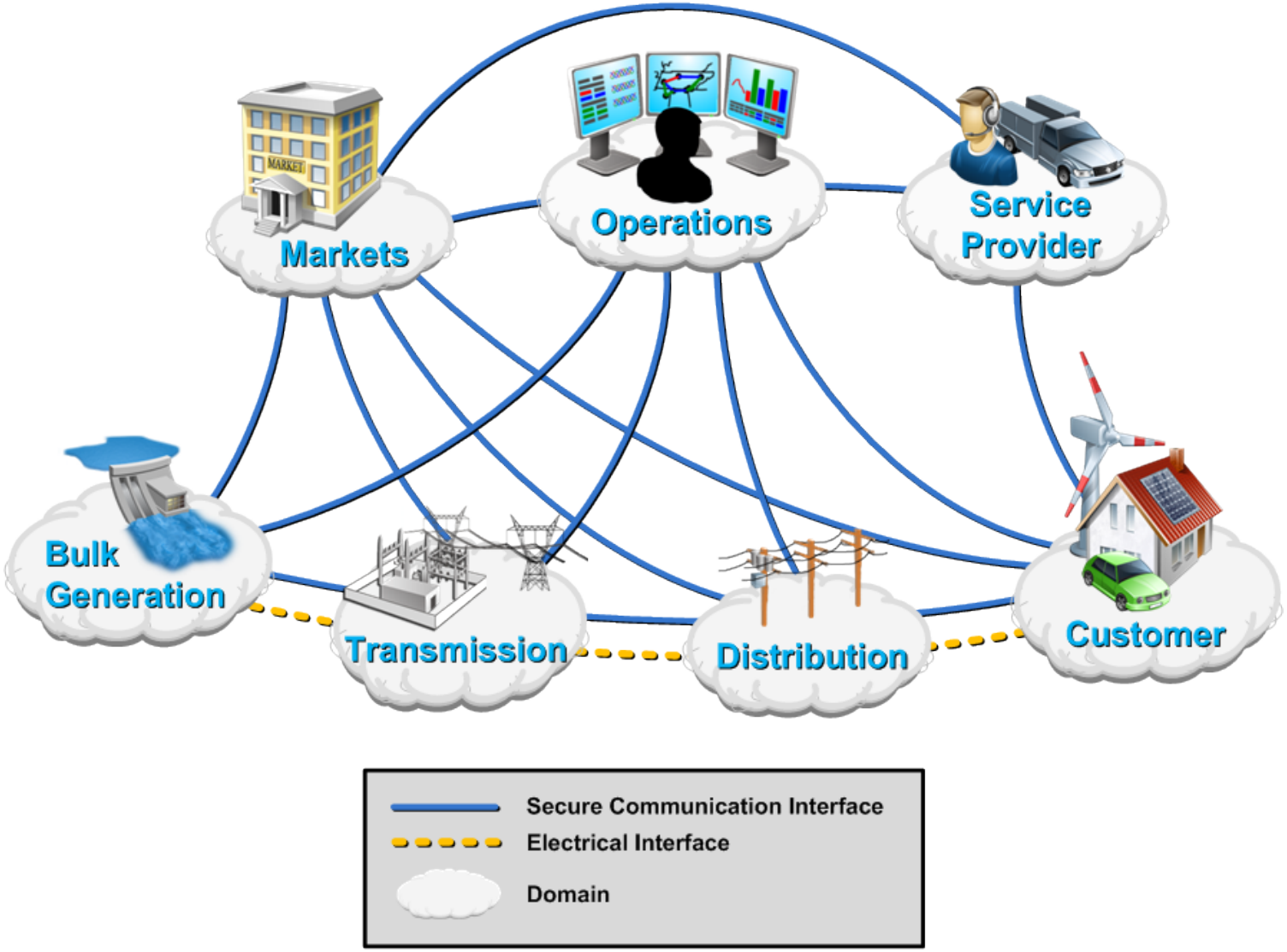
Pulling back the curtains to reveal the front battle lines of Smart Grid security.

Justin Searle – InGuardians

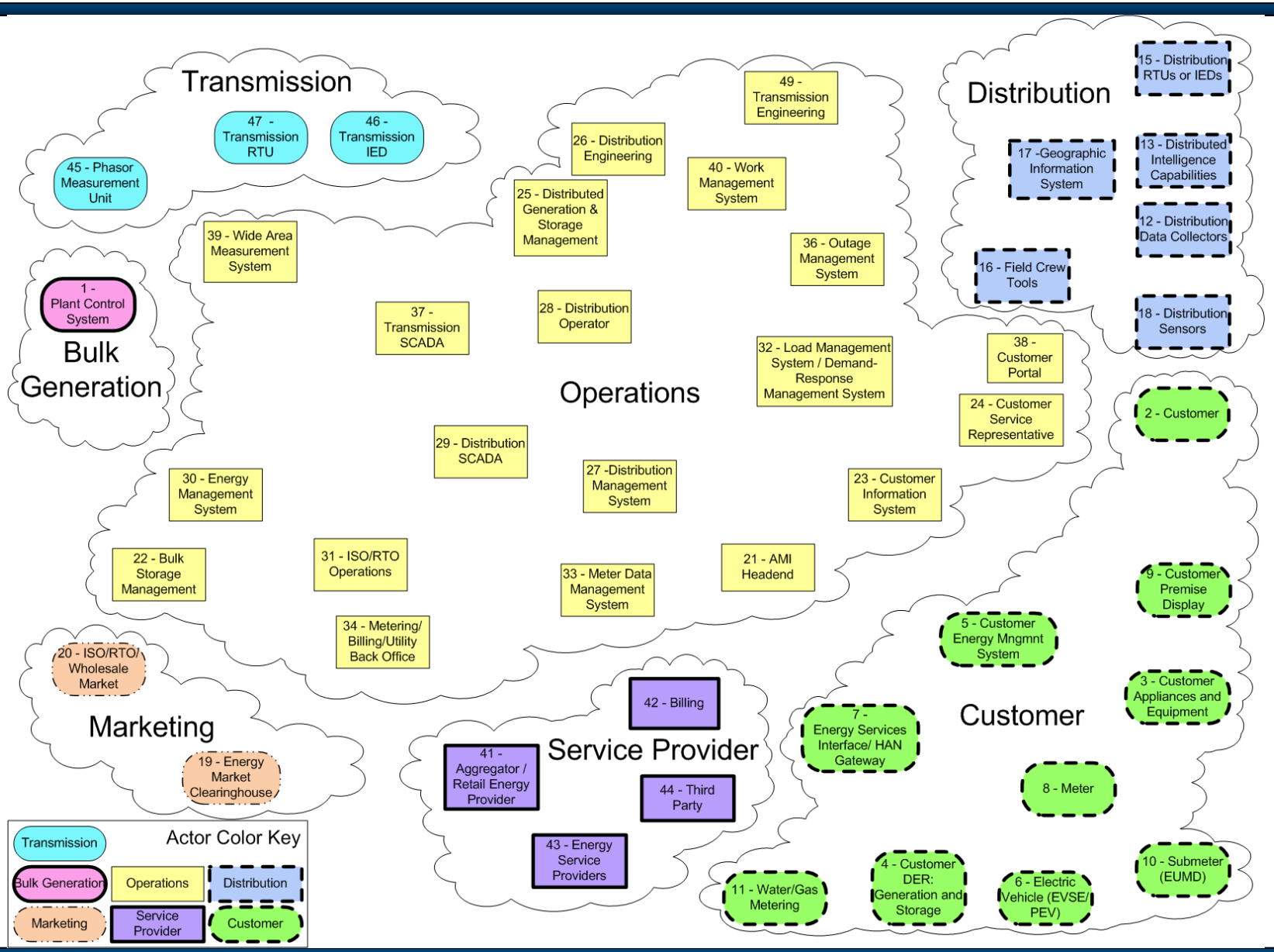
Types of Security Assessments

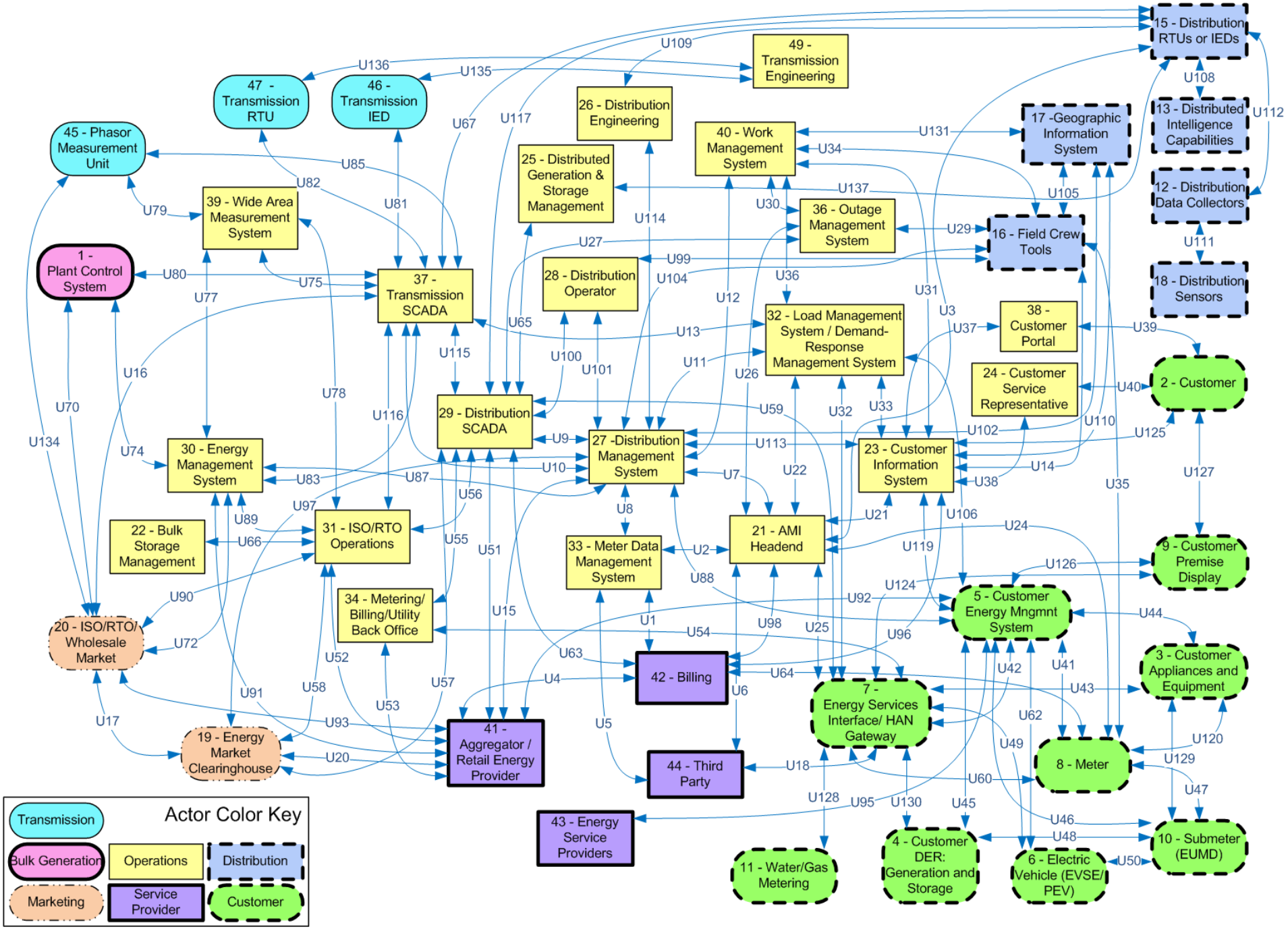
- Best Practice Assessments / Security Architecture Reviews:
  - Focuses on engineer/admin interviews to evaluate security posture
  - Looks at system implementation and configuration
- Vulnerability Assessment:
  - Focuses on the use of automated tools, often with some degree of manual verification
  - Looks for known system vulnerabilities and mis-configurations through the use of vulnerability signatures and system versioning
- Penetration Testing:
  - Focuses on the arts of system misuse and reverse engineering
  - Utilizes the concept of attack and pivot to identify difficult-to-discover vulnerabilities several layers deep
  - More accurately gauges the risk of known vulnerabilities
  - Requires a higher degree of technical expertise and knowledge
    - Extensive manual efforts
    - Custom tool creation

Smart Grid Conceptual Model

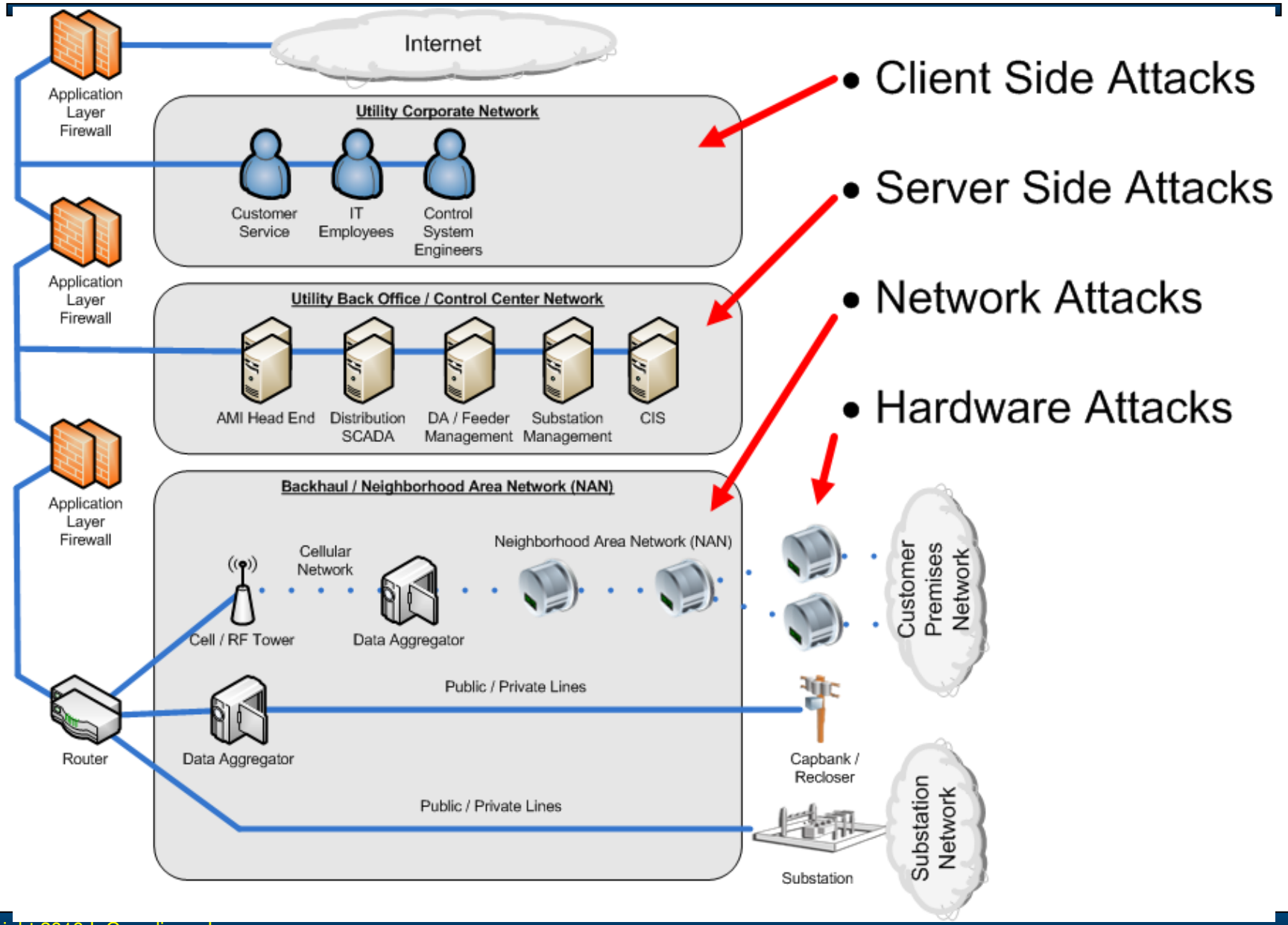


Smart Grid Reference Model - Domains





Basic Utility Attack Surface



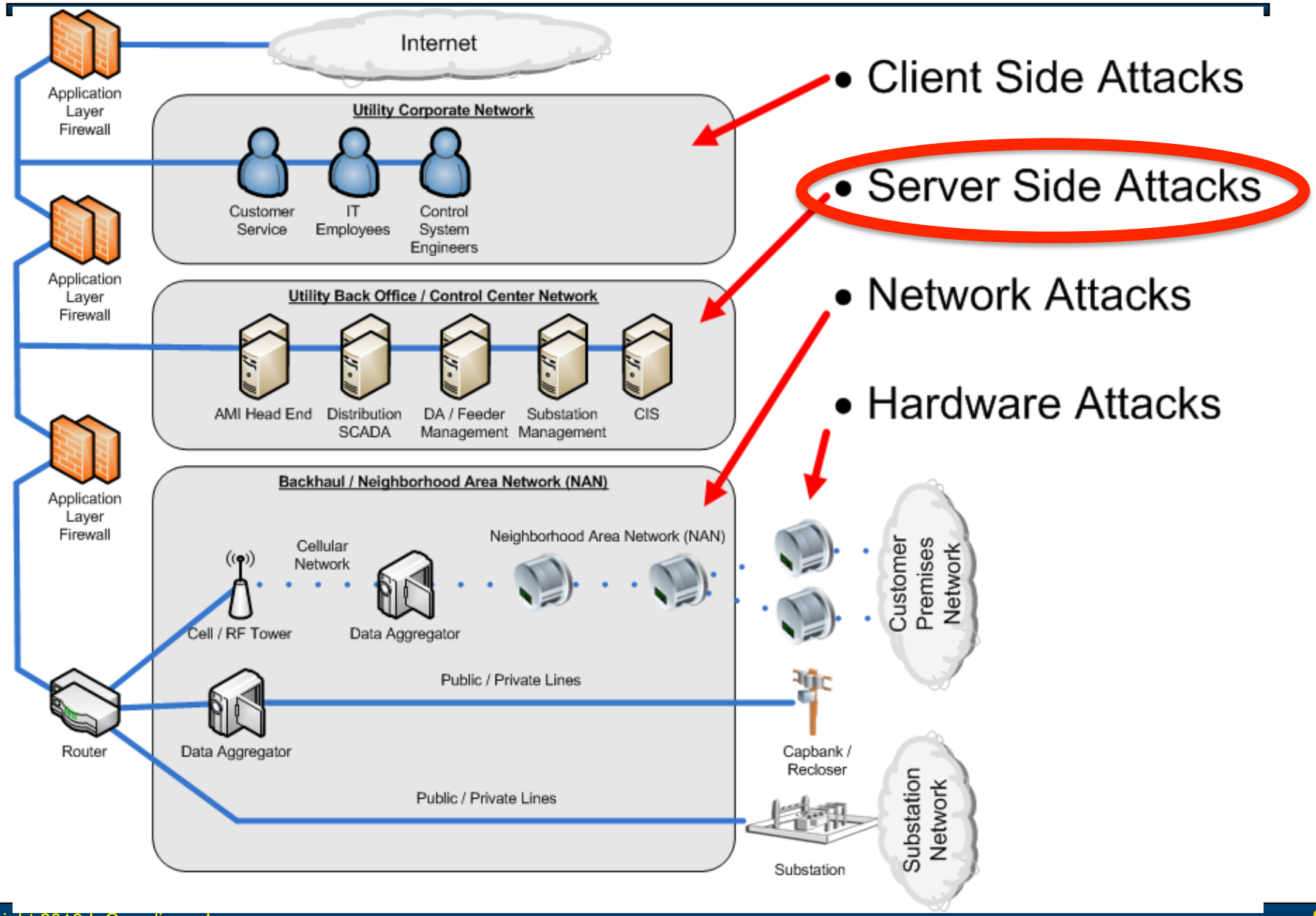
Client Side Attacks

- For years, attackers have been leveraging company workstations as a primary attack avenue
  - Perimeters are getting harder to attack directly
  - Employees are more dependent on the Internet
  - Web browsers have excessive functionality that can be used for both good and evil
  - Employees have access to company's internal systems
- Types of client side attacks:
  - Malware, Viruses, and Botnets
  - Software vulnerabilities via buffer overflows, security boundaries, and software update mechanisms
  - Web browser attacks such as XSS (Cross Side Scripting) to execute malicious code on a user's browser

Client Side Defenses

- Traditional defenses are of limited use against targeted attacks
  - Antivirus can be bypassed within minutes through binary repacking and modification
  - Bypass web proxy filters by using non-blacklisted sites
- Network segregation and properly implemented access control provide the strongest and most economical defense
  - Limit access to sensitive data and control system functionality
  - Segregate sensitive workstations and servers from other systems
- What does this mean for Utilities?
  - Prevent customer service reps from issuing disconnect/reconnect and demand response signals. Have it go through a ticketing system to a smaller control systems team
  - Deny Internet access to all workstations that issue control signals or interface with control systems, such as control center workstations, AMI administrators, and employees approving disconnect/reconnect and demand response signals

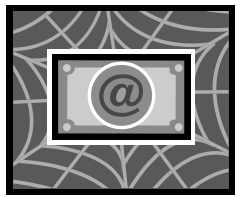
Server Side Attacks



Server Side Attacks

- Customer and Employee portals are obvious targets
- Attacks on internal servers from compromised workstations should also be expected
- Pivoting through internal user web browsers to attack internal web applications is far less obvious
  - Most web applications are vulnerable to CSRF (Cross-Site Request Forgery) attacks
  - CSRF attacks are completely transparent to the user and can affect any system they are currently logged into
  - CSRF attacks don't require compromised workstations
- It is critical to understand web based attacks like CSRF because most of our Smart Grid systems use web based management interfaces

Cross-Site Request Forgery (CSRF)



Employee opens a second tab and surfs to the Attacker website (or MySpace page…)

2

3

Hidden in the page, the Attacker's website tells the employee's web browser to disconnect a customer's power

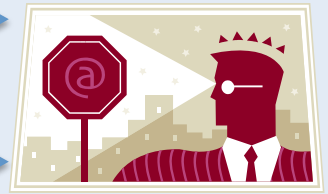
Attack Prerequisites

- Attacker must have knowledge of the application he is attacking (can be obtained at conferences)
- Attacker must know the hostname or IP address of the CIS system (can be obtained by browser based attacks)

Utility Network

1 Employee using CIS system throughout the day

4 Web browser sends disconnect request to CIS

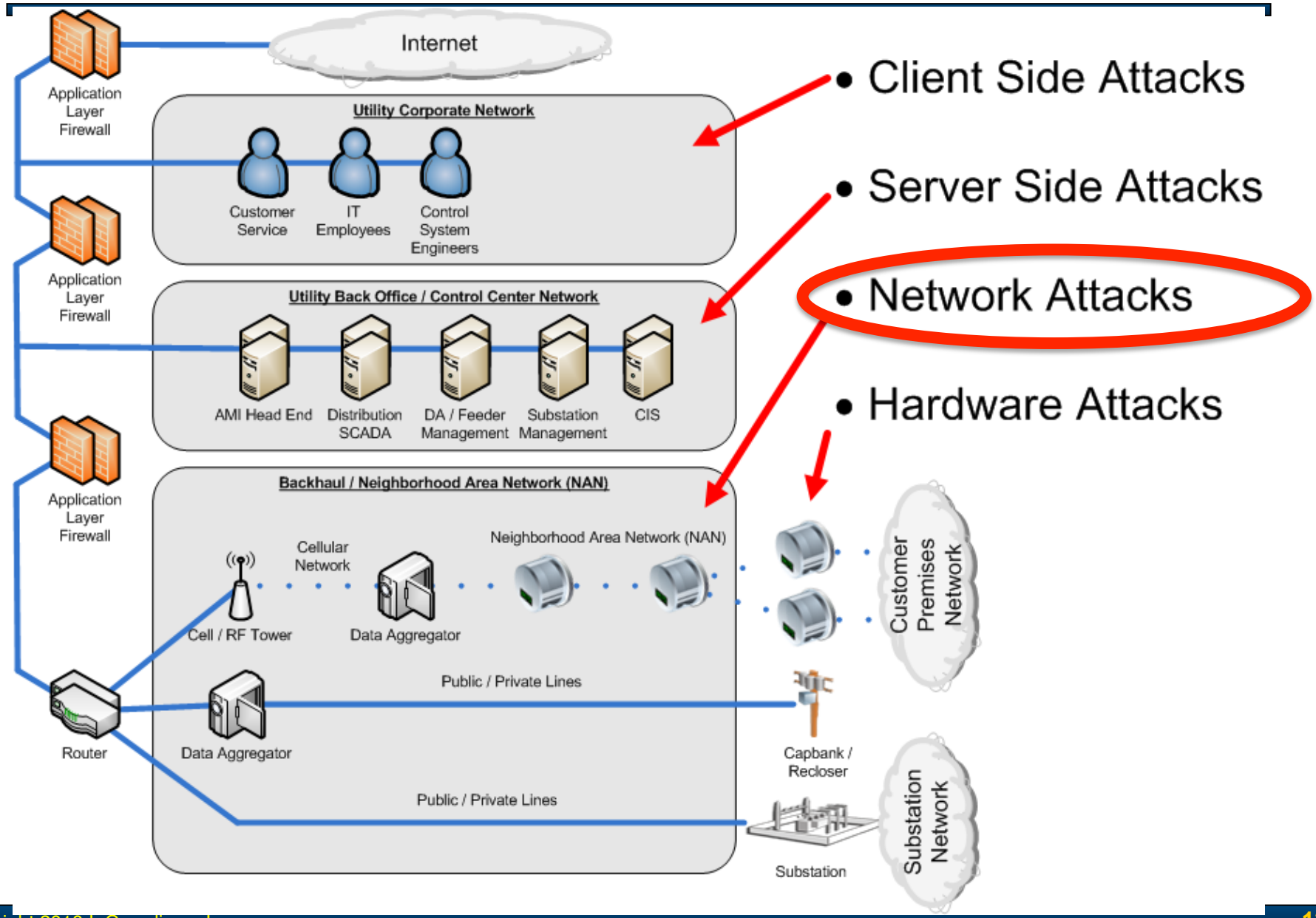


Customer Information System with Power Disconnect Capabilities

Server Side Defenses

- Keep systems patched and updated
- Perform periodic vulnerability assessments and penetration tests
- Use Intrusion detection and intrusion prevention systems in strategic positions around highly sensitive servers and control management systems
- Utilize centralized logging systems for alerting and forensic evidence

Network Attacks



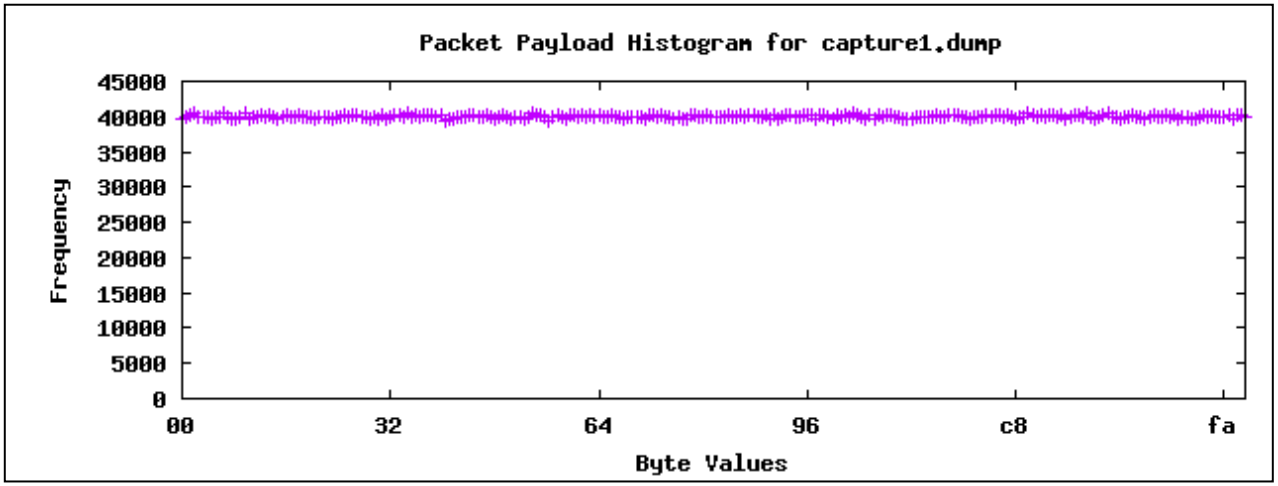
Network Protocols and Security

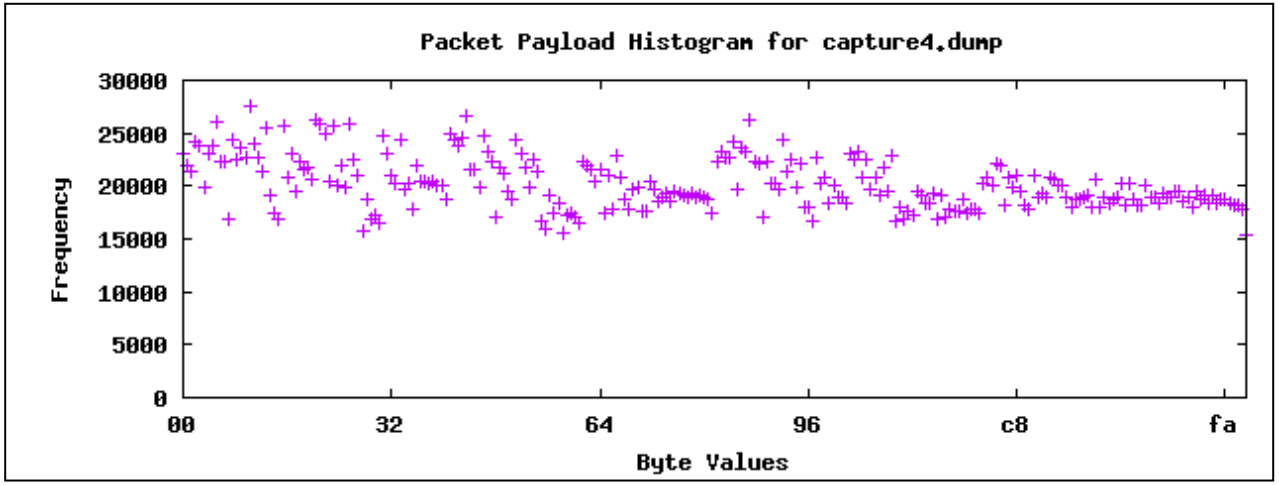
- Its pointless to compare proprietary protocols to standards based protocols from a security perspective
  - standards based protocols benefit from greater transparency, but suffer from "interoperable" hacker tools
  - proprietary based protocols benefit from obscurity and sparse hacker tools, but suffer from limited security reviews
  - the same arguments can be made for open source vs. proprietary software
- Securely architected protocols is essential, but properly implemented and configured protocols are just as important

Attack: Weak Cryptography

- Many proprietary systems implement their own cryptography
  - Some create their own crypto algorithms
  - Others create their own crypto stacks of know algorithms
  - Just because it's "AES" doesn't mean it's secure
- Exploits in insecure cipher modes, weak nonce construction, IV re-use, etc…
- Practical attacks include replaying data, decrypting packets, key recovery, data manipulation / injection
- Analysis tools to test implimentations: Ent, visualization of RNG's, cryptographic accelerators, custom scripts

Histogram Analysis





Insecure Block Cipher Modes

- AES ciphers using CTR mode effectively become a stream cipher
- Without key derivation and rotation, IV collisions compromise integrity of cipher

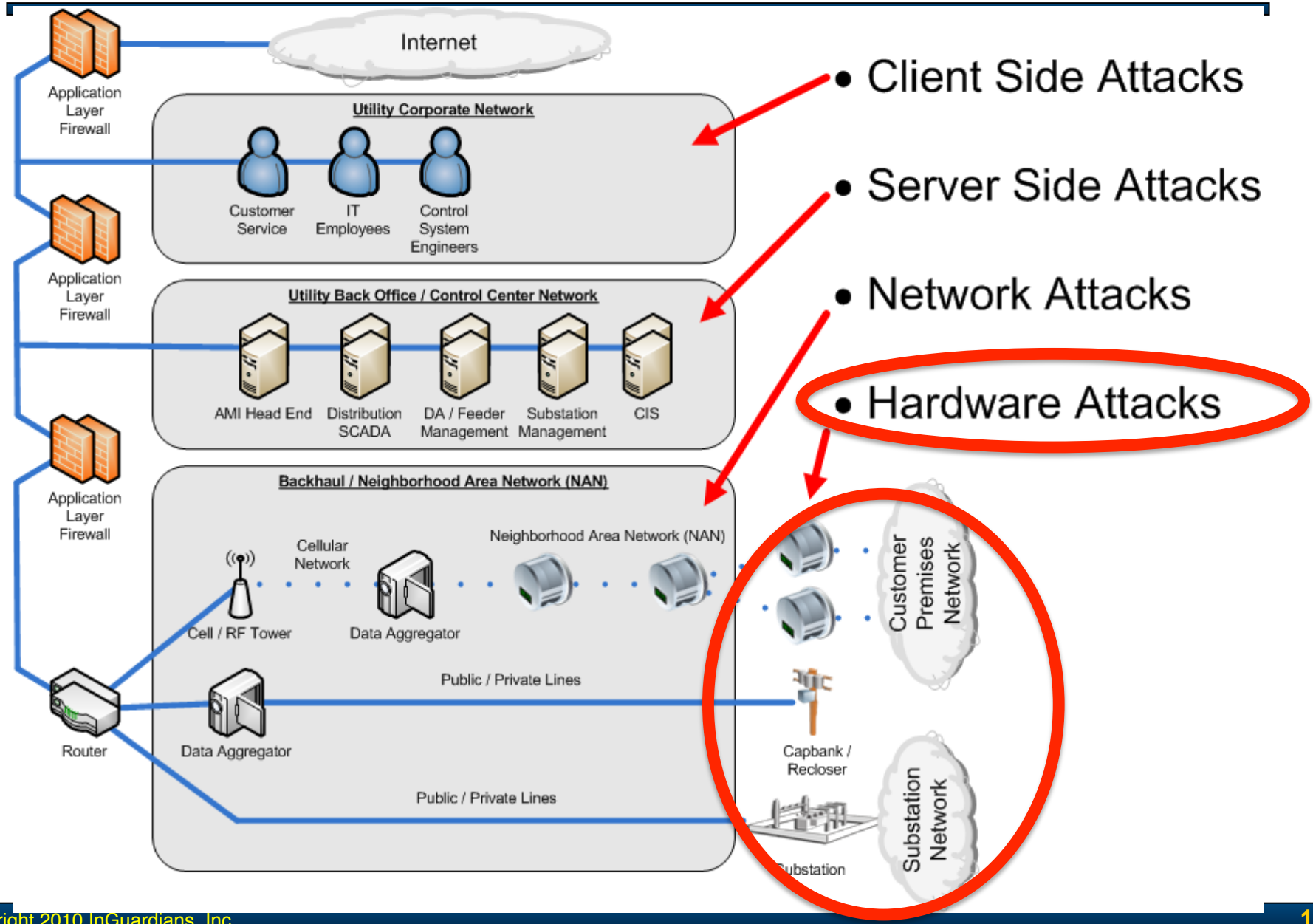
```
C:\>type ivcoltest.py
#!/usr/bin/env python
knownplain = "\xaa\xaa\x03\x00\x00\x00\x08\x00\x45\x00\x01\x48\x00\x01\x00\x00"
knowncip = "\x31\xb9\x84\x81\xe1\x96\x6e\x71\xd8\xa3\x39\x0c\xfb\x48\xaa\x61"
unknowncip = "\x31\xb9\x84\x81\xe1\x96\x6e\x71\xd8\xa3\x3d\x0c\xfb\xb5\xaa\x61"
print "Decrypted packet: "
for i in range(0,len(knownplain)):
    print "%02x"%( (ord(knownplain[i]) ^ ord(knowncip[i])) ^ ord(unknowncip[i]) ),
print("\n")

C:\>python ivcoltest.py
Decrypted packet:
aa aa 03 00 00 00 08 00 45 00 05 48 00 fc 00 00
```

Defense: Weak Cryptography

- Design and implementation of cryptographic systems is extremely difficult
  - Avoid this if possible
  - Leverage vetted third-party encryption stack implementations
- If necessary, model system after proven protocols
  - IEEE 802.11i RSN key derivation
- Expert cryptographic review consulting

Vulnerabilities in crypto are especially hard to recover from (remember WEP?)

Hardware Attacks



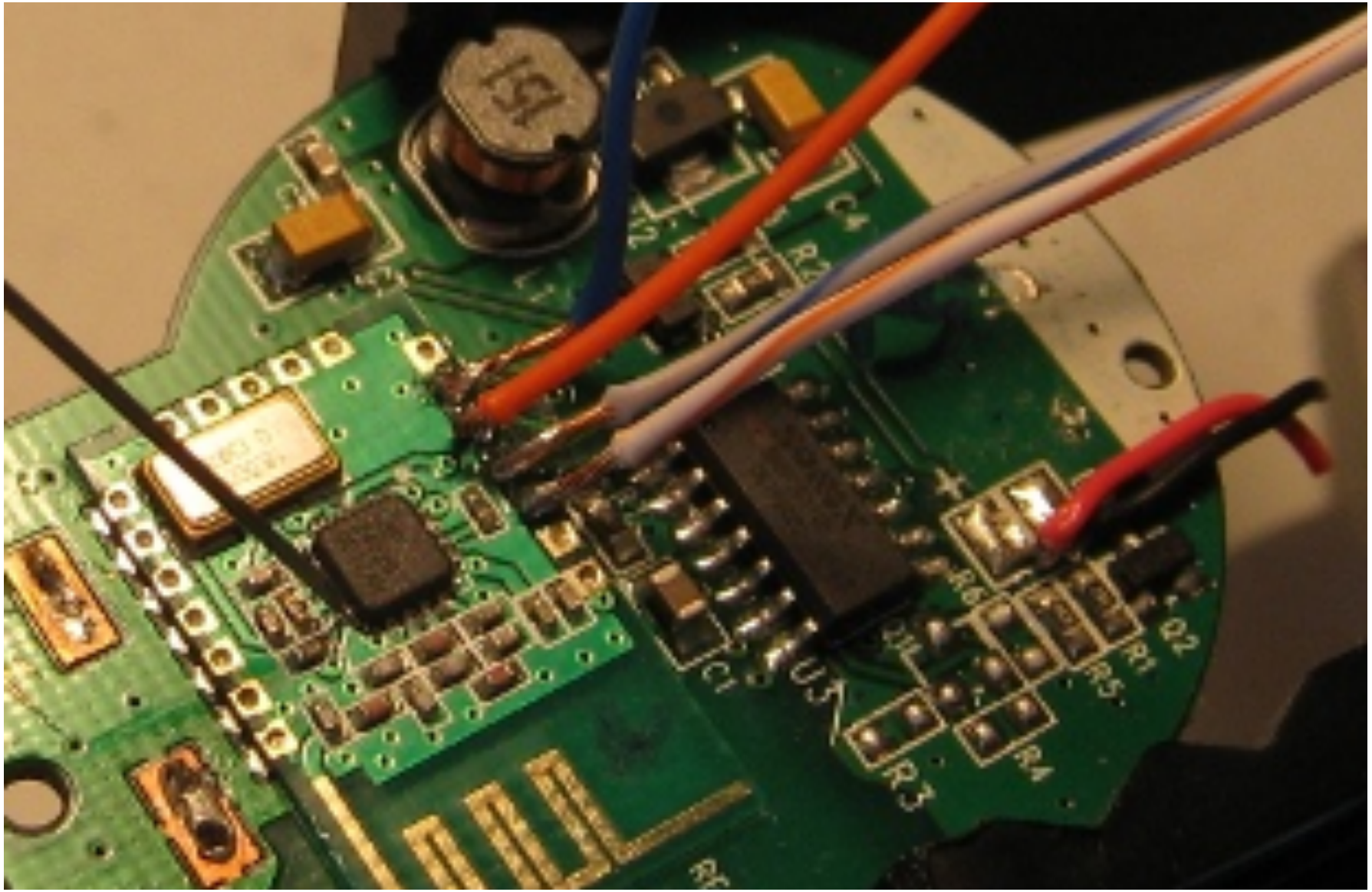
Hardware Attacks

- All field deployed devices are susceptible to physical hardware attack
  - Meters on residential homes are obvious targets
  - Pole-top devices such as DA and feeder automation devices are not much harder to access (albeit riskier to health)
  - Substation physical defenses are a deterrent, not an insurmountable obstacle
- If tamper mechanisms or perimeter alarms are triggered, modified hardware is not easily detected
- Basic Hardware Attacks:
  - Encryption key and flash extraction
  - Firmware / Software vulnerabilities
  - Flash image manipulation

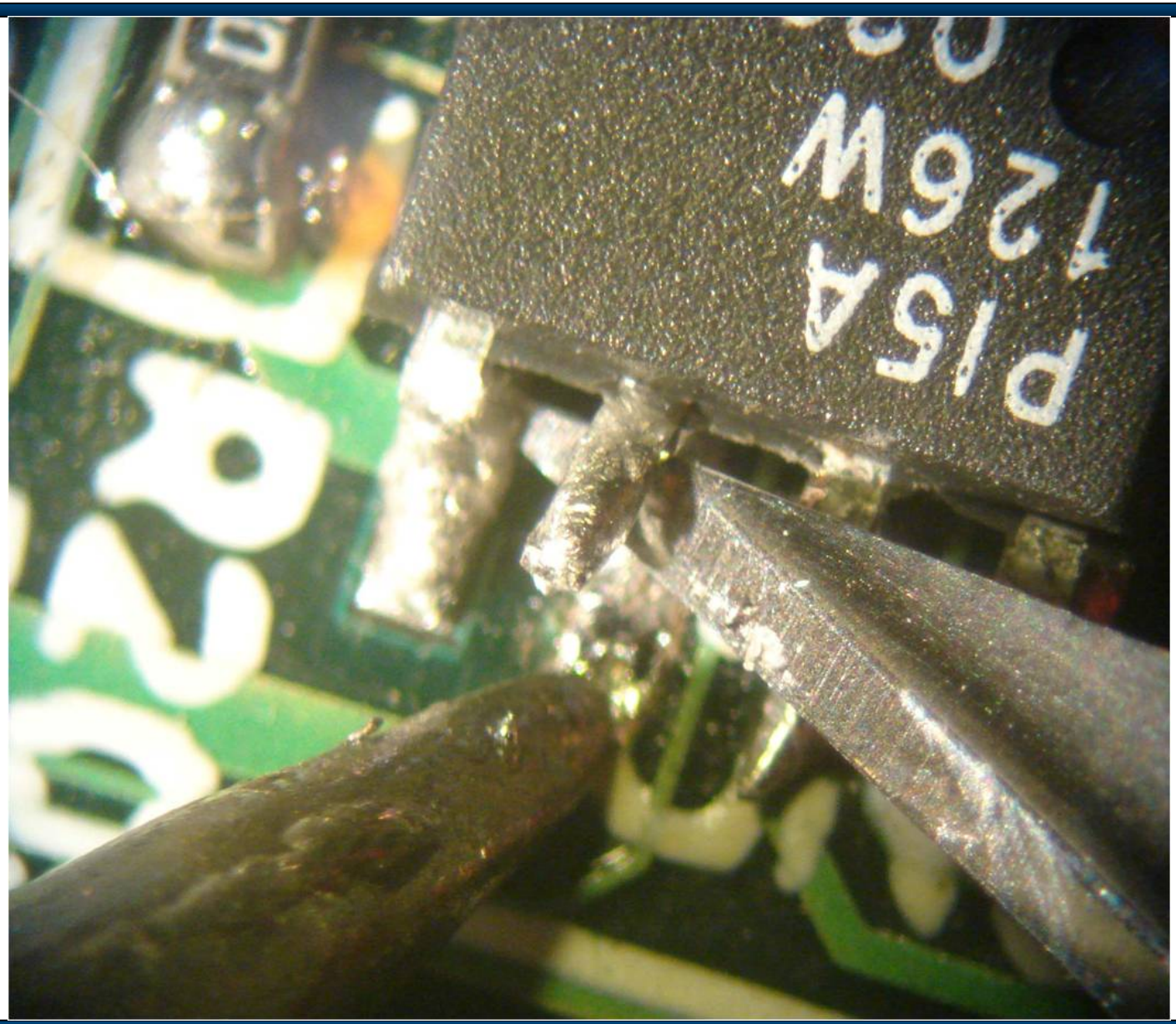
Attack: Key & Firmware Extraction

- Extract locally stored encryption key and firmware
  - Extract contents of RAM, Flash, and EEPROM data
  - Identify encryption key or firmware
  - Especially useful when a single key is shared across multiple devices
- Intercepting data between circuit board peripherals
  - Operate and boot device normally in a lab, monitoring bus activity between major chips (MCU, Radio, EEPROM, RAM)
  - Identify encryption key or firmware
    - Encryption key can often be found in key load operations between a microcontroller and crypto accelerator
    - Firmware can often be found in software updates between radio and flash

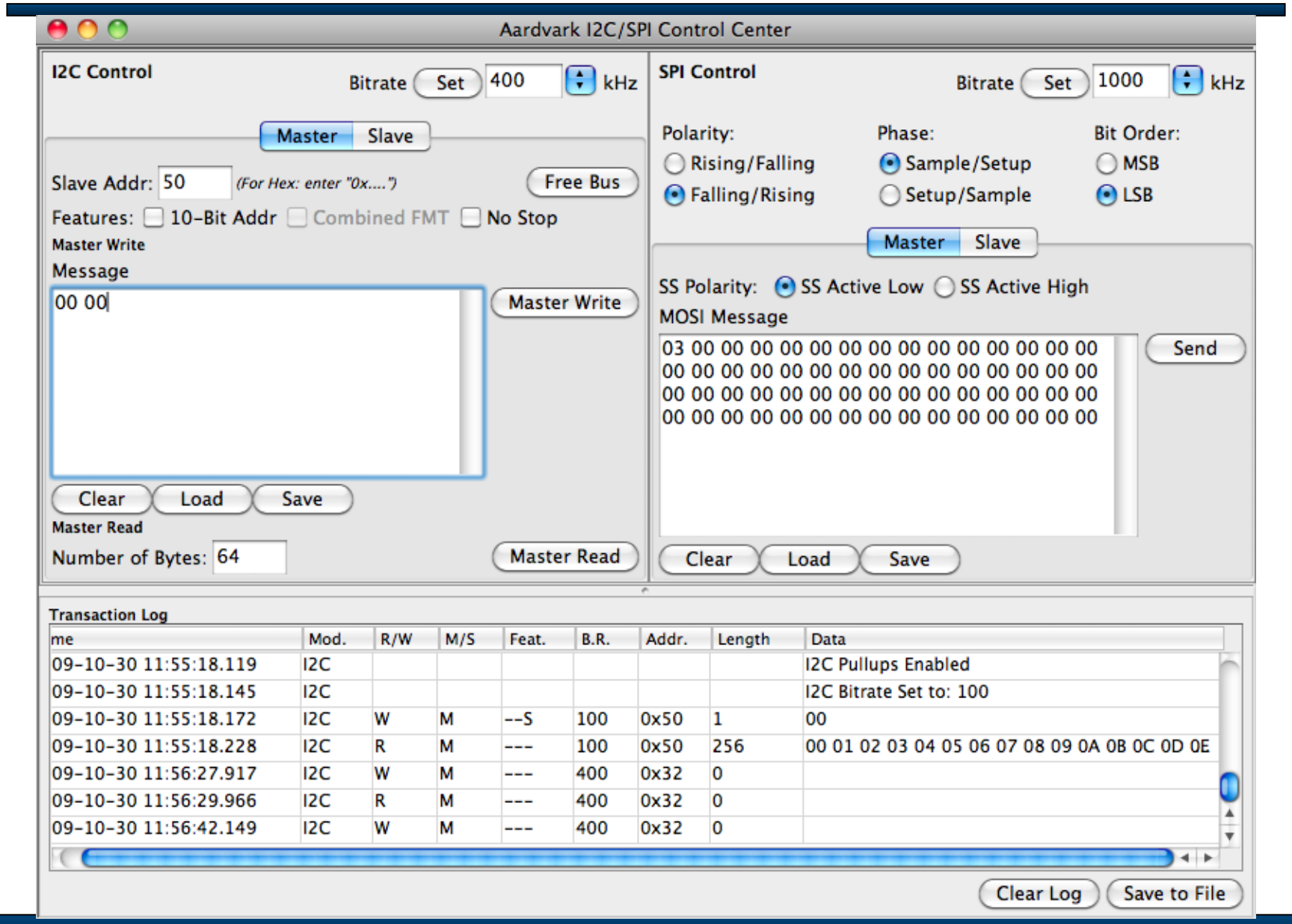
Interfacing with an IC



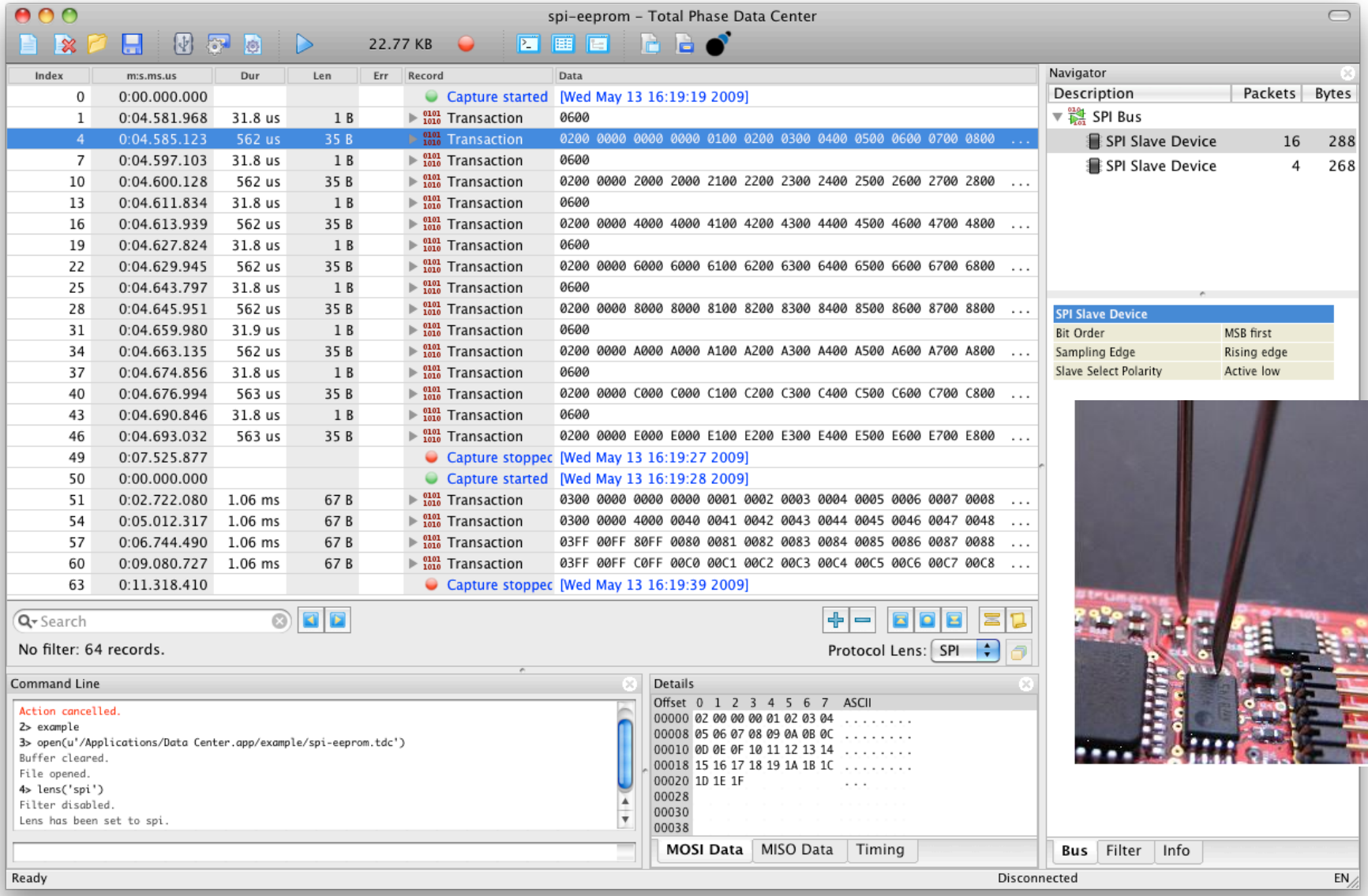
Lifting an IC's Chip Enable (CE) Pin



I2C EEPROM Dumping



SPI Bus Snooping



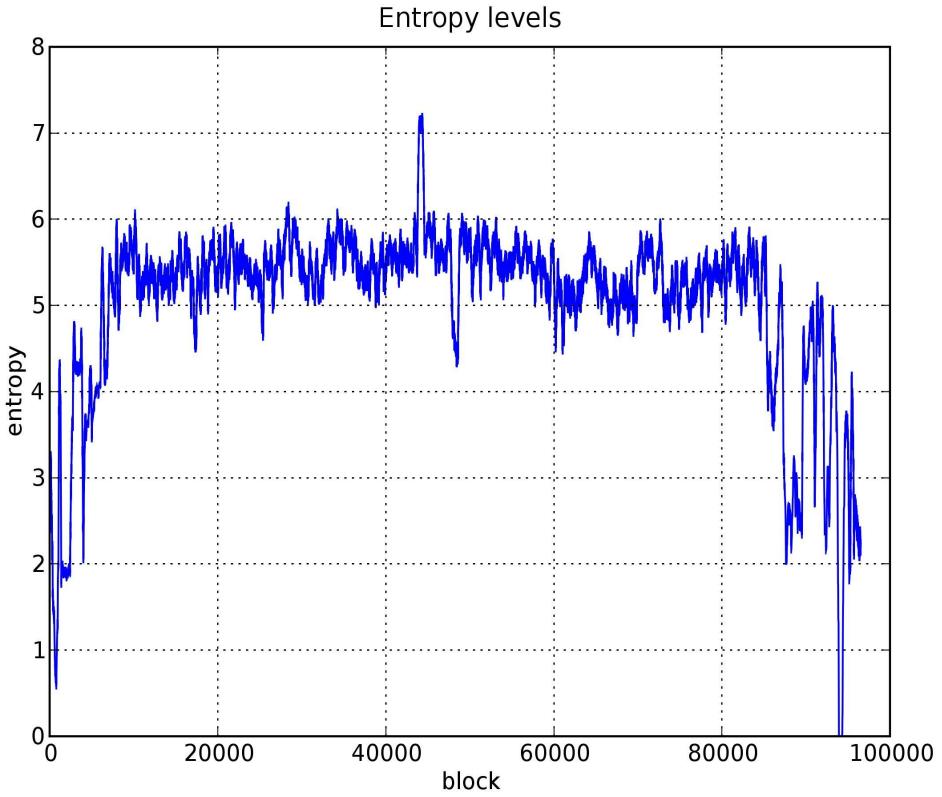
Symmetric Key Search

- Basic string searches for obvious keys
- Develop custom tools to do more advanced searches:
  - GoodFET: Abuses vulnerability in TI, Ember radios to access RAM even when chip is locked
  - zbgoodfind: Search for ZigBee key using RAM dump as a list of potential keys
  - Combined they can recover the ZigBee network key

```
$ sudo goodfet.cc dumpdata chipcon-2430-mem.hex
Target identifies as CC2430/r04.
Dumping data from e000 to ffff as chipcon-2430-mem.hex.
...
$ objcopy -I ihex -O binary chipcon-2430-mem.hex chipcon-2430-mem.bin
$ zbgoodfind -R encdata.dcf -f chipcon-2430-mem.hex
zbgoodfind: searching the contents of chipcon-2430-mem.hex for
encryption keys with the first encrypted packet in encdata.dcf.
Key found after 6397 guesses:  c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc
cd ce cf
```

Asymmetric Key Search

- Asymmetric keys have high entropy (very random)
- RAM and Flash is filled with non-random data
- Graphing entropy of flash reveals a spike in randomness
- This spike is the location of the asymmetric key in flash



Defense: Key & Firmware Extraction

- Utilize System-on-a-Chip (SoC) devices when possible
- Hardware tamper-proof mechanism and monitoring
  - Learn from Microsoft, epoxy layers are only a speed bump
- Limit encryption key distribution to small groups of devices, preferably with unique keys per meter
- Obscure encryption key storage
- TPM's can protect asymmetric keys
- Implement key rotation mechanisms

Be prepared to answer: What is my remediation strategy once the encryption keys protecting the NAN are compromised?

Conclusion

- Required skills for assessing Smart Grid security cover many areas
  - Hardware, software, wireless, cryptography and more
- Through efficient testing, we can address vulnerabilities before they threaten deployments
- Publically available AMI Attack Methodology
  - Download it at www.inguardians.com
  - An InGuardians created document funded by the original ASAP (AMI Security Acceleration Project) project
  - Provides a detailed methodology for performing penetration tests on smart meter networks
  - Methodology can be adapted for Feeder automation and Substation networks

Contact Information

Justin Searle
justin@inguardians.com
801-784-2052

www.inguardians.com