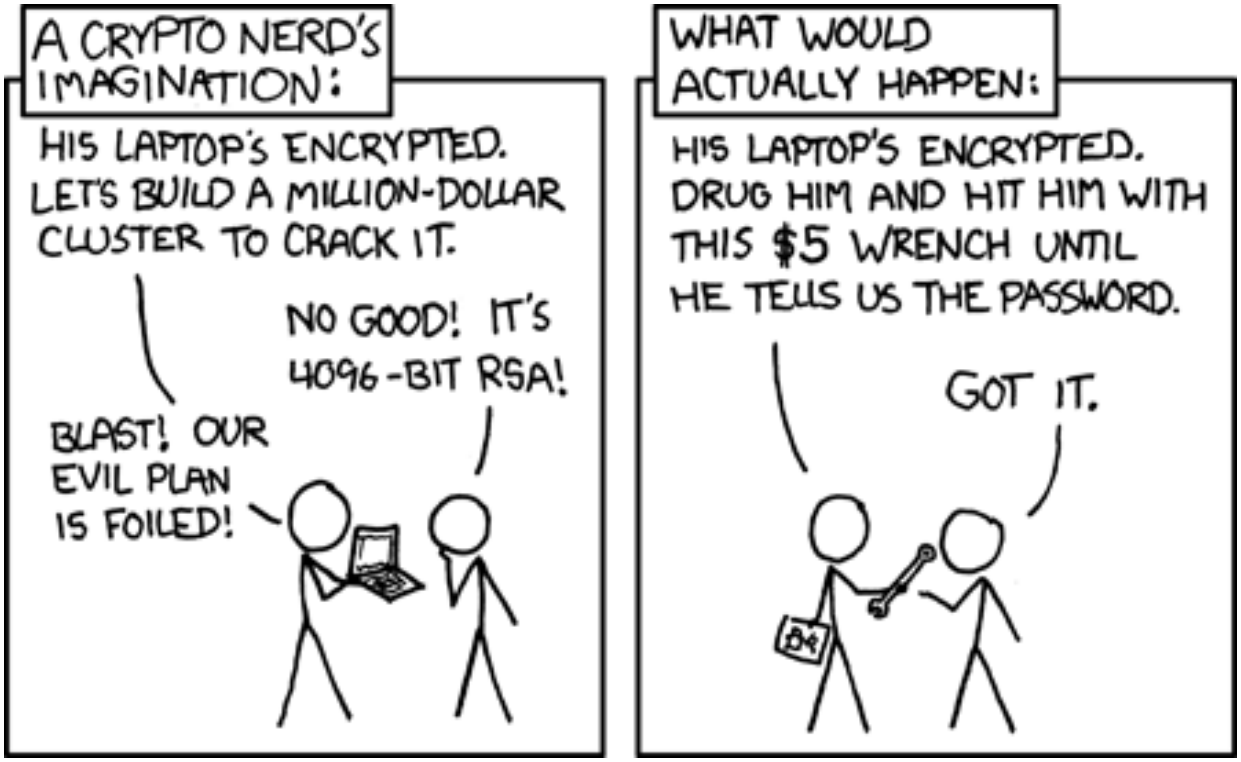
Keys In A Hostile Work Environment

IEEE Key Management Summit 2010

Marc Massar, CISSP-ISSAP, NSA-IAM

How Cryptanalysis Really Works



From xkcd - http://xkcd.com/538/ Used in accordance with Creative Commons Attribution-NonCommercial 2.5 License

Hostile Work Environment – It's not what you think

- Kerckhoffs' Principle
  - Fewer secrets means less brittle – breaking security
- Adversarial Relationship with the protected device/data/keys/etc
- Limited Communication with endpoint
- Diverse Environments
  - Deployments might be inconsistent even for very similar devices/functions/processes

Candidate Environments

- End-to-end encryption in the payment industry
- TPM Chips
- Smart Cards – EMV, authentication cards (PIV/CAC), Cable/Satellite
- Remote data gathering systems – Predators, bomb devices, communications systems

End-to-End Encryption

End-to-End, Point-to-Point, Left-to-Right, whatever you want to call it. I'm just surprised Adidas hasn't come after all the E2EE vendors yet.

End-to-End Encryption Payment Environment

- Diverse – especially in retail
  - Hardware is different
  - Networks are different (if they even exist)
  - Software is different
  - Some hardware standards for key protection – varying implementations though
- Limited Communication – how do you communicate with a device that's connected by a serial cable?
  - Stand alone
  - Integrated
- Adversarial – Bad Guys want magstripe, PINs, PANs, and more!

TPM Chips

Did you hear the one about the guy who subverted the potting, EM shielding, side-channel protections, and a bunch of other crazy stuff with an electron microscope and some needles? Where's MacGyver when you need him?

TPM Chips

- Diverse – Not as bad as other candidate environments
  - There are standards here
  - Implementations can vary greatly
  - Uses are different too
- Adversarial – Again, the bad guys want what you have, and it's sitting right there
  - TPM chips protect things like FDE (full disk encryption), biometric authentication, and others
  - Expect targeted attacks against
- Limited Communication – It's sort of one-sided
  - TPM chips are "write only"

“Smart” Cards

How smart can they be when the data that is protected gets passed around in the clear?

Smart Cards

- Adversarial – the bad guys have what they want (they just can't unlock it)
  - Cards are skimmed or stolen
  - Value is guaranteed in possession
- Limited Communication – once deployed it's hard to talk to the device – especially when disconnected
  - Payment cards don't get updated
  - Prox cards (for example) aren't going to get updated by a door sensor
- Diversity – less diverse than they once were
  - Multiple standards
  - Still implementations leave much to be desired (EMV offline example)
  - Multiple use cases drive different requirements for key management (authentication, data protection)

Remote Action Systems

Information gathering, bomb defusing, or saving the leaders of the human resistance – when this guy gets captured do you really want the enemy to be able hack his authentication scheme?

Remote Action Systems

- Adversarial – Units get deployed "in theater"
  - Not just adversarial – hostile and dangerous
  - Devices go where humans can't or shouldn't because of risk
- Limited communication – what happens when the device gets out of range?
  - Communications get cut – or tapped
- Diverse systems – communication units are often integrated in very different devices
  - Crypto has been deployed here for years
  - What is actually being protected?

Now What?

I think maybe I need to go back to shiny gold keys I can see instead of
1101001101010110010111010011010101101010110101100101101010101011111000010100110010111010001111010010001010110010100000011110111

How to address conditions

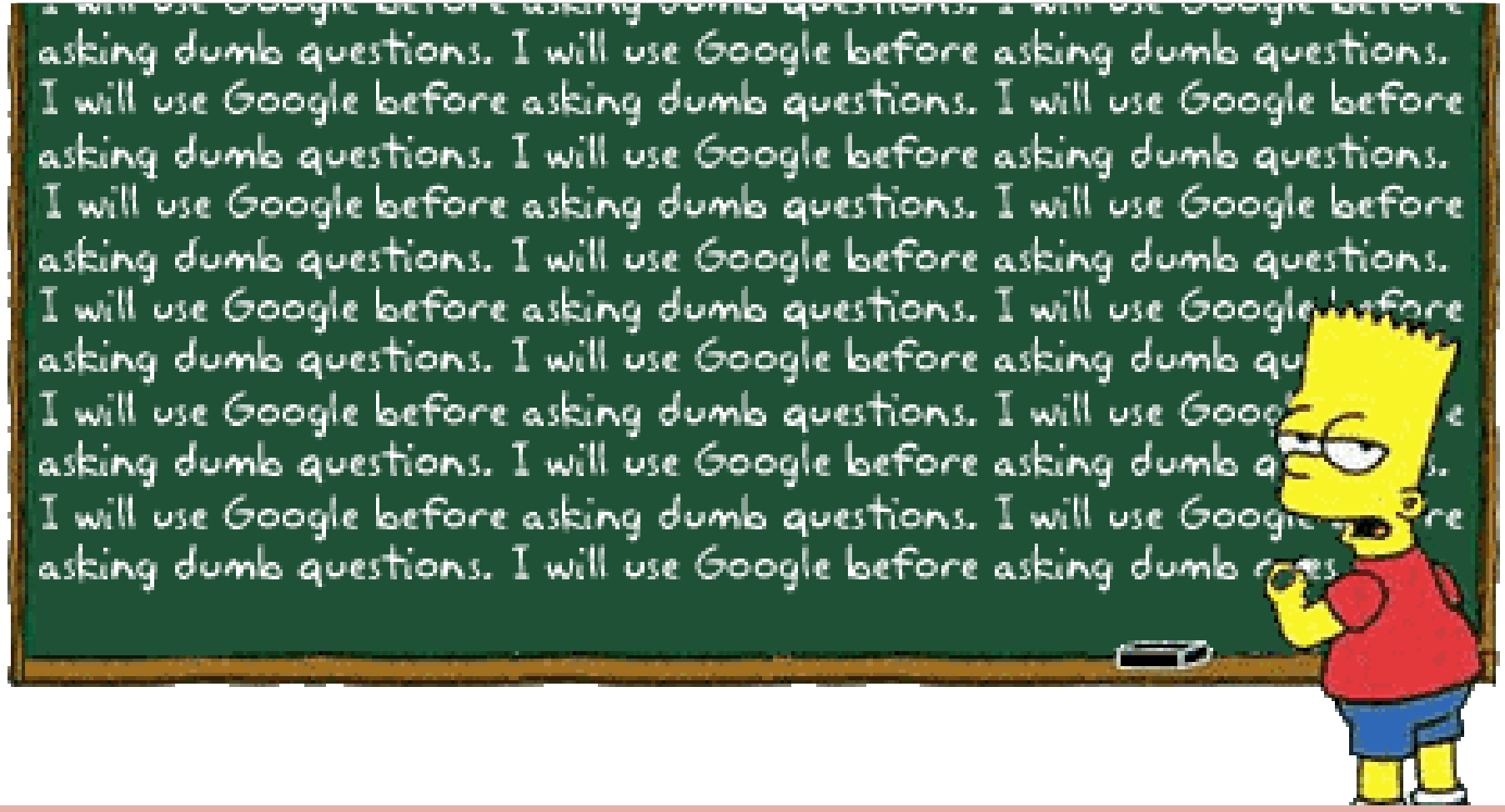
- Diversity
  - Make things less diverse – duh!
  - Simpler security architectures are less brittle
  - Think about operational considerations
- Adversarial
  - Devalue the data
  - Improve data owner awareness
  - Make it harder to get at data (keys or real data)
- Limited Communications
  - Embed key protocols in regular communications
  - Build separate protected channels
  - Shrink what you have to send/receive

How to address conditions

- Standards
  - Need to consider diverse deployments
  - What are the use cases where the standards “don’t fit?”
  - Can we make them fit?
  - Build in support for limited communications
- Derivation schemes
  - Exchange public information rather than key material
- Asymmetric schemes
  - Beware Trust issues

Brittle Security vs. Resilient Security

- Simple – Complex
  - NIST – SP800-27 – Principle 24 “Strive for Simplicity”
- Useable – Secure
  - NIST – SP800-27 – Principle 15 – “Strive for operational ease of use”



Questions?