Attacks on Cryptoprocessor Transaction Sets

Mike Bond, Proc. of the CHES 2001 Workshop, LNCS 2162, Springer-Verlag, 220-234.

Presented By: Fuad Tabba

Cryptoprocessors and Transaction Sets

- A separate tamper-resistant processor to handle sensitive data
- No publicly known physical attack
- Transaction sets are the processor's interface to the world
- Provide the commands to manipulate and manage the information
- Users are restricted by roles to a subset of these commands

No single individual should be able to compromise the system

My Evaluation

- Looks at the system from a holistic point of view (Security as a process not a product)
- Lays down the fundamentals of the attacks before going into the implementation (Properly sets the scene)
- Does not discuss the implementation of two of the attacks (why?)

Would recommend reading up to section 4.

Security is a Process

- A chain is only as strong as its weakest link
- It is the interfaces that are often the least secure part
- Transaction sets are the weakest link
- A single corrupt individual is able to compromise the system – without needing to attack the hardware!

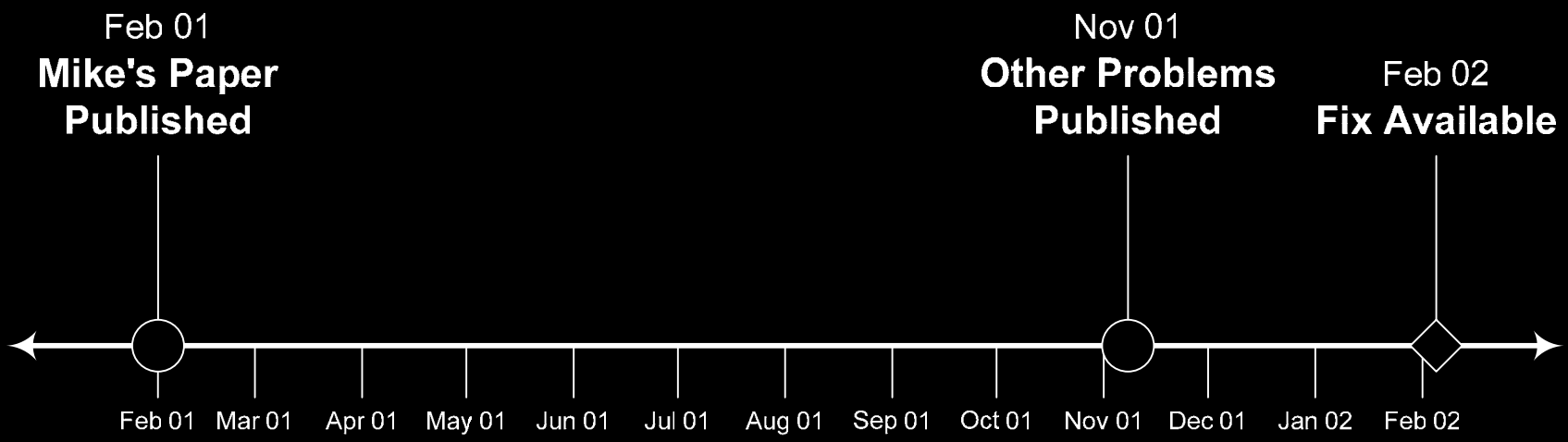
Why break the front door when it's easier to jump through the window?

Setting the Scene

- Explains how the attacks work in "*The Attacker's Toolkit*":
  - Meet in the Middle Attack
  - Related Key Attacks *
  - Unauthorized Type-Casting
  - Poor Key-Half Binding
  - Conjuring Keys from Nowhere *
- Implementation of the attacks builds on this section

** Practical implementation not discussed*

Is it ethical to publish a system's vulnerabilities before they have been fixed?



"*…no single individual can damage the integrity of the key material [any more].*"