Updating Shannon's Maxim

Jay Jacobs

Target Corporation

Agenda

- My World of Cryptography
- Look back: Updating Shannon
- Why there is a problem: Study
- What now

Jay Jacobs

- OASIS KMIP TC
- ISSA
- Key Management, PKI
  - Medical Devices to Retail
- Internal Consulting (Detective/Translator)

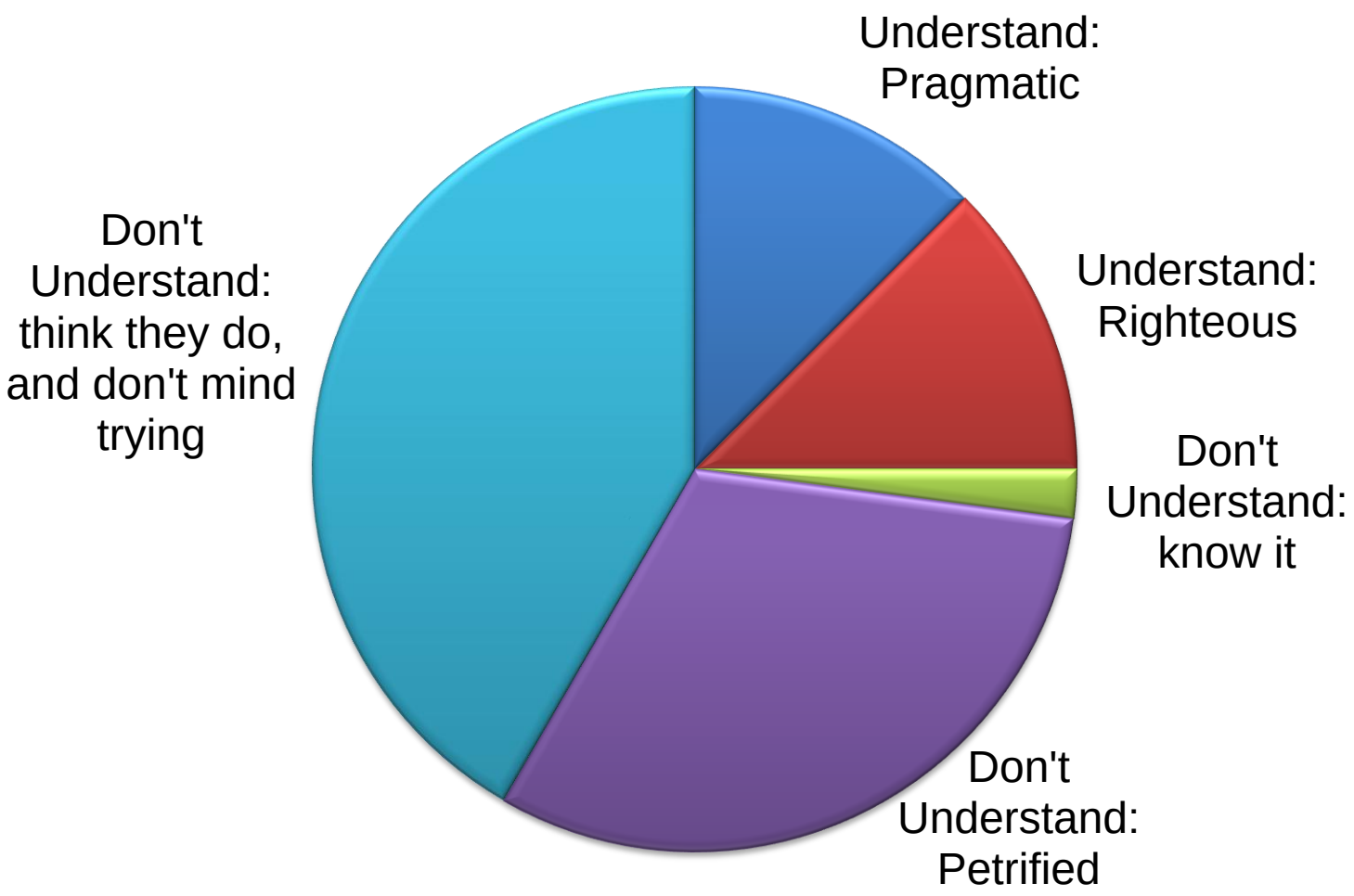
Example: “Certificate Problem”

Q: Does the server authenticate the client (mutual SSL auth)?

A: No. We use standard public/private key for SSL certificate.

Study: World of Cryptography

(informal, almost scientific approximation of values)



Don’t mind trying…

```
//obfuscate data.
for (curPos=0; curPos < plainTextLen; curPos++) {
   cipherText[curPos] = plainText[curPos] + *(secretKey+keyIndex++);
   if (keyIndex >=secretKeyLen)
        keyIndex = 0;
}

#define OBFUSCATION_KEY       “xyzzy"
```

Looking back

“It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.”

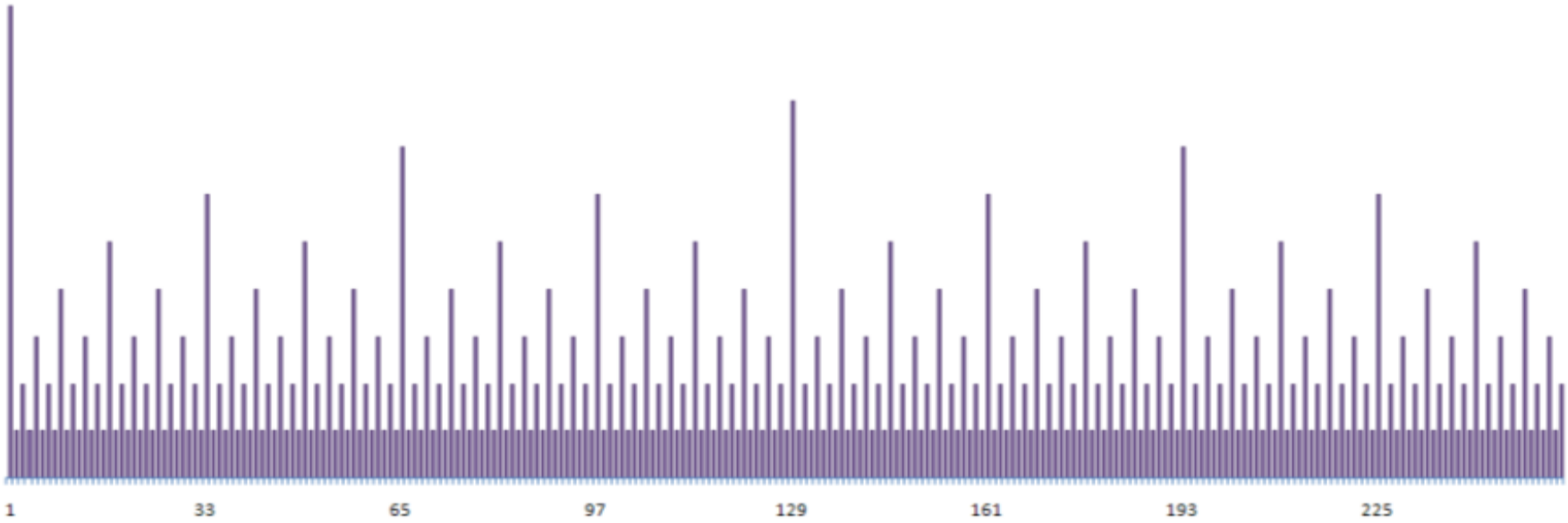
-- Auguste Kerkhoffs

“The enemy knows the system.”

-- Claude Shannon

The enemy knows key derivation

“The key seed is used to mathematically select from a set of random numbers, and is used to change those random numbers into new numbers, guaranteed to be unique”



Updating Shannon

The enemy knows the system,

and the allies do not.

…and the allies do not

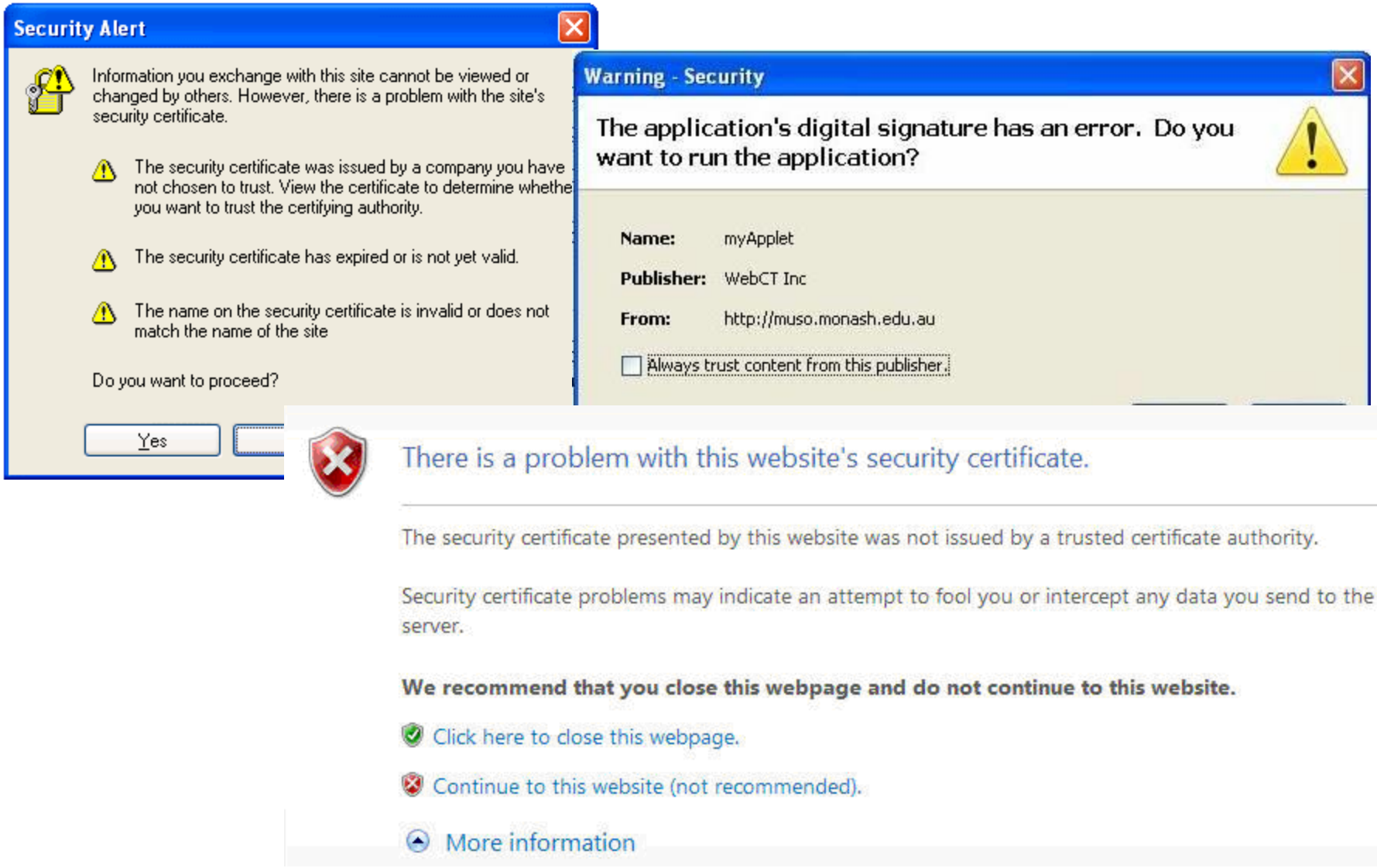
Is this okay?

[Our] software employs multiple encryption algorithms in succession to guarantee that the resulting “Token” can never be decrypted.

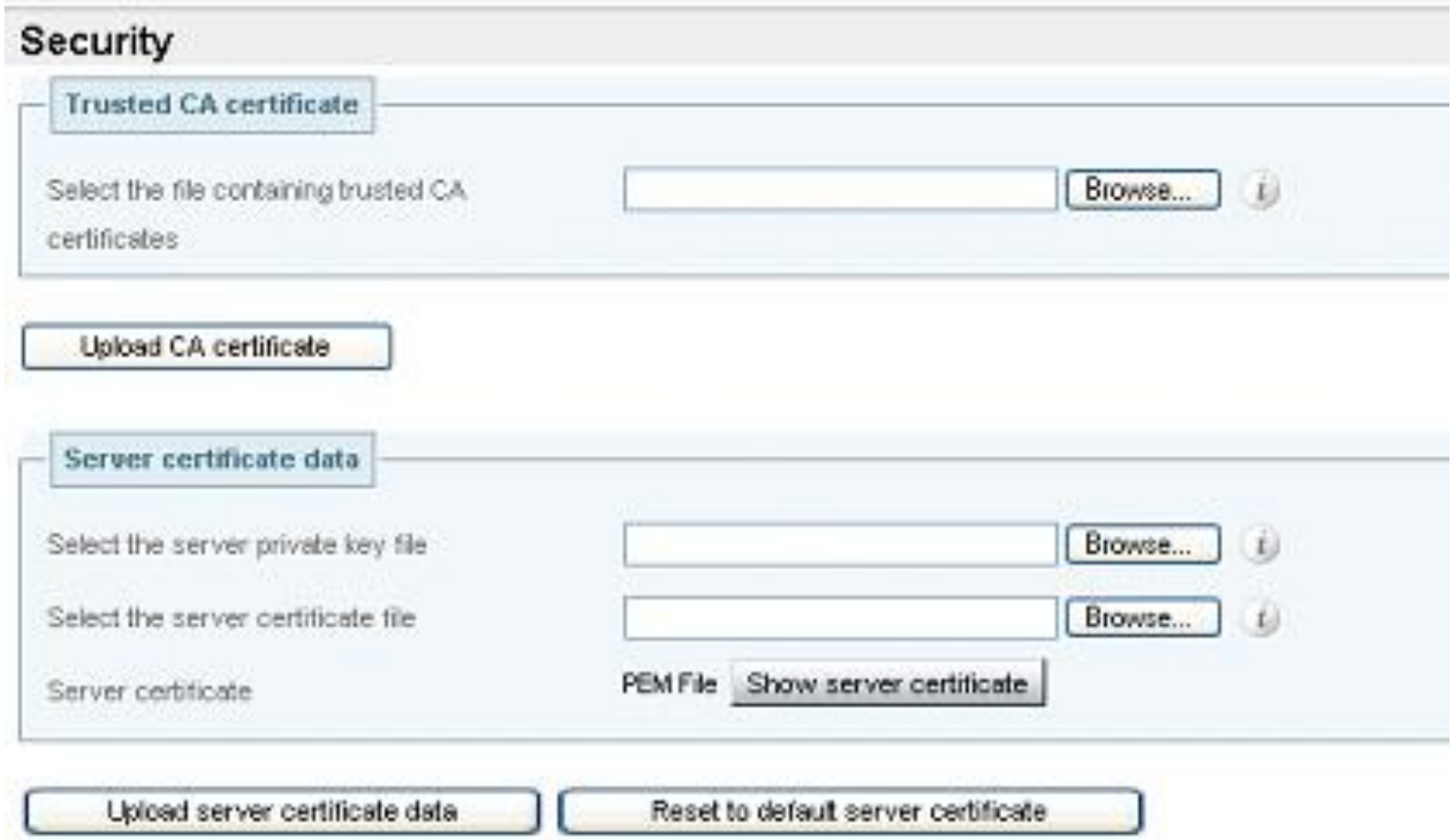
The encryption algorithms used include Secure Hash Algorithm-256 (SHA-256).

Once all data elements have been encrypted as described above, the entire file is encrypted using … a 64-bit private key block cipher.

Between Design and Use



Identify the Design Flaw



Manifestations

2010 UK Security Breach Investigations Report:

Listed “poor server configuration/authentication” as the second most prevalent vulnerability leading to a compromise.

2009 Verizon DBIR:

“error during deployment and routine administration of systems was the leading category of error contributing to data compromise”

Error listed as a contributing factor in 67% of the breaches investigated.

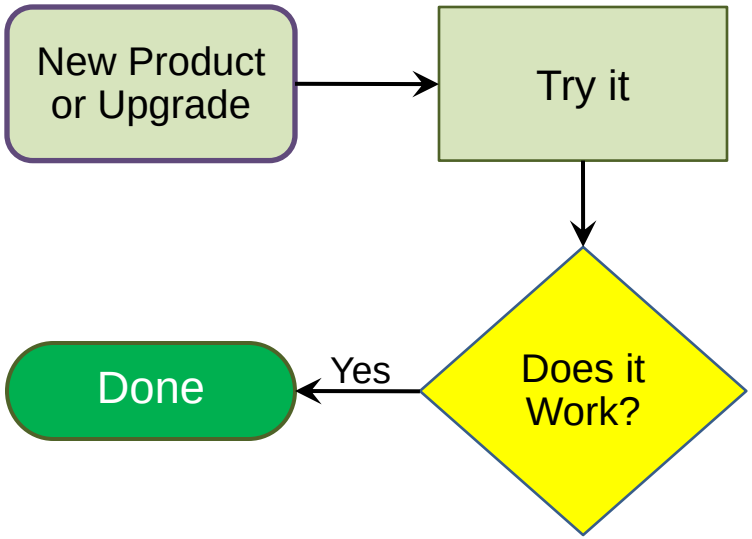
Consumer Cryptography

- There is no basic or easy cryptography
- It’s all about motivation
- KM server vs. KM client motivation
- The need for pragmatic cryptography

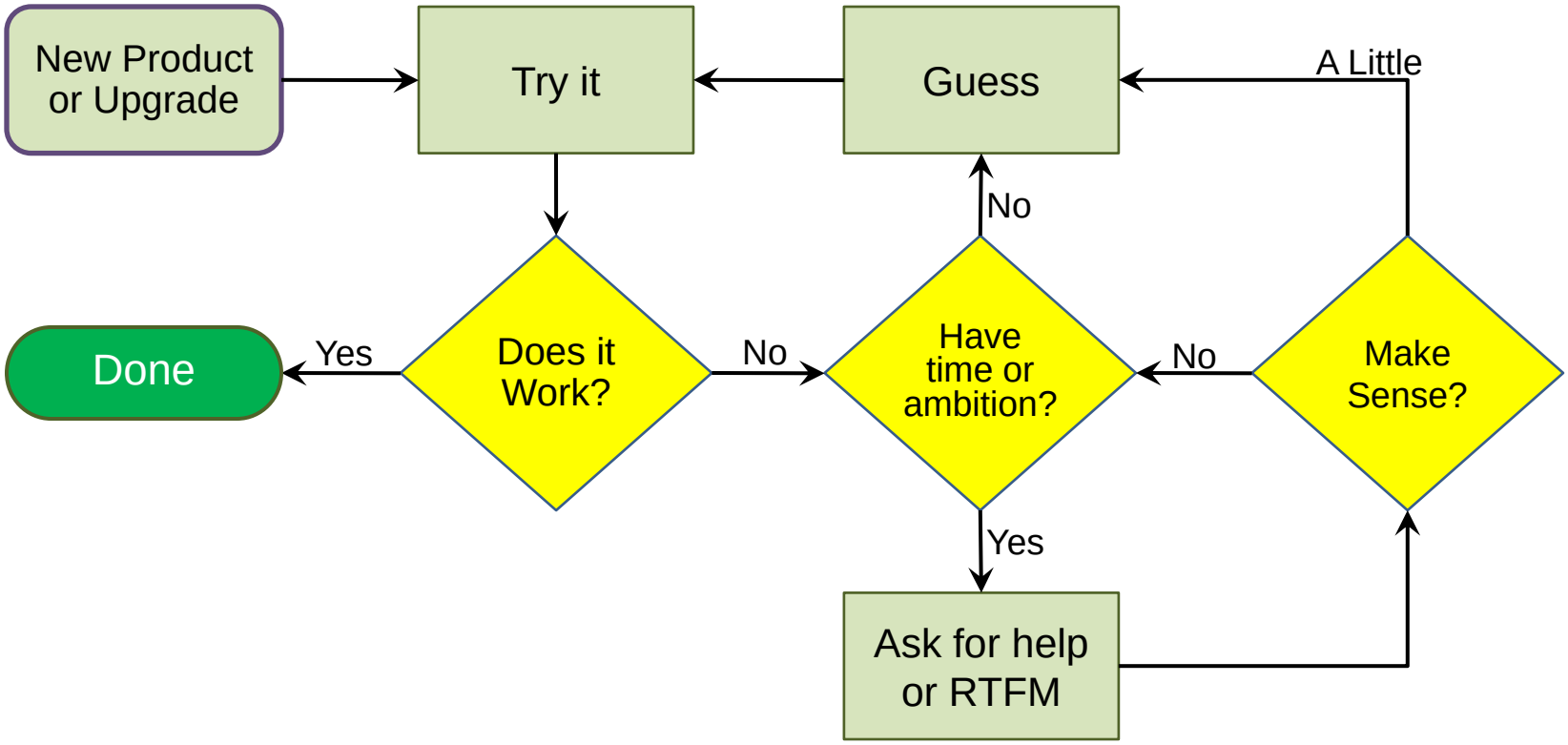
Why a new maxim is needed

An empirical study of the rituals performed by the “allies” during installation and maintenance

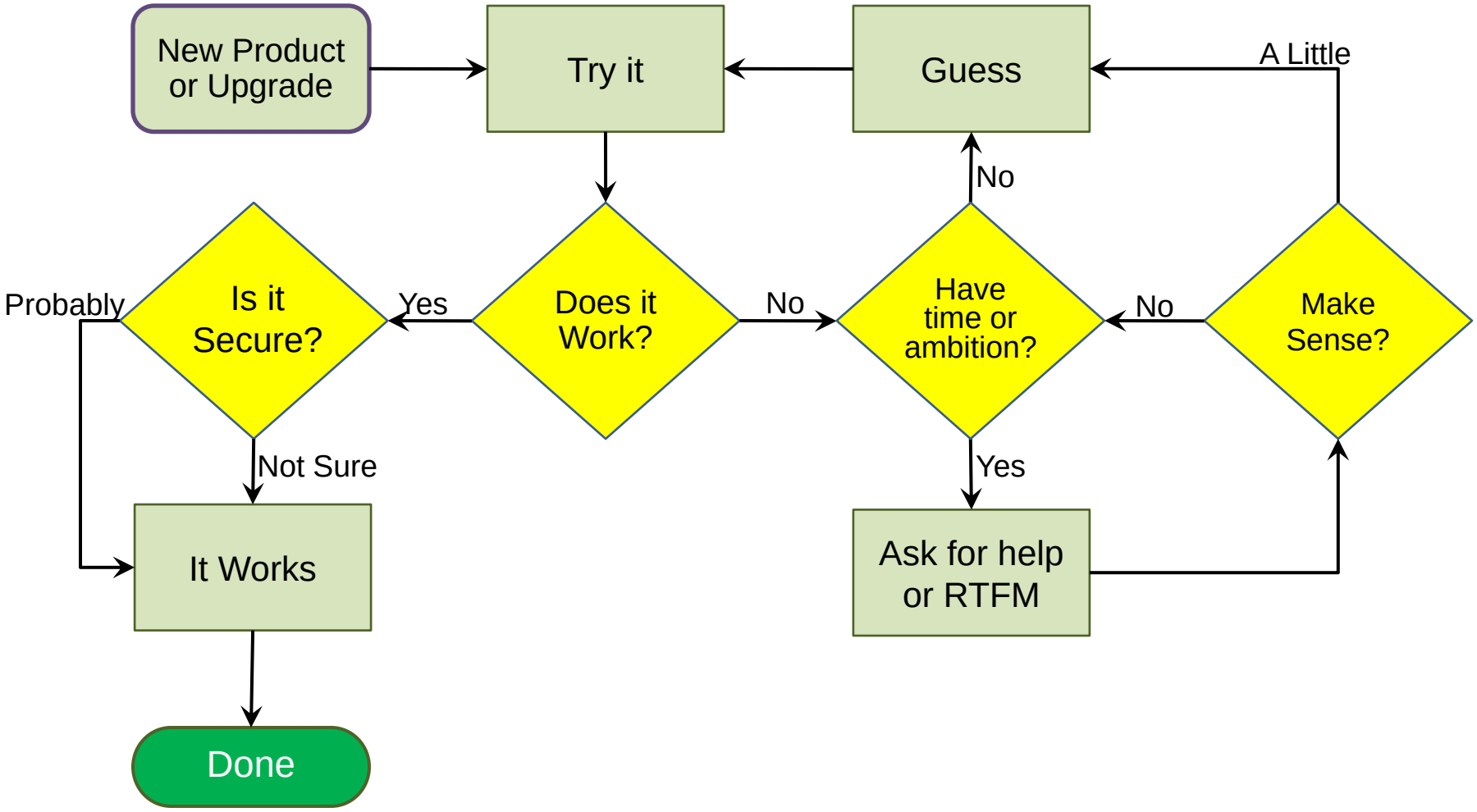
Typical Process Flow



Full Process Flow

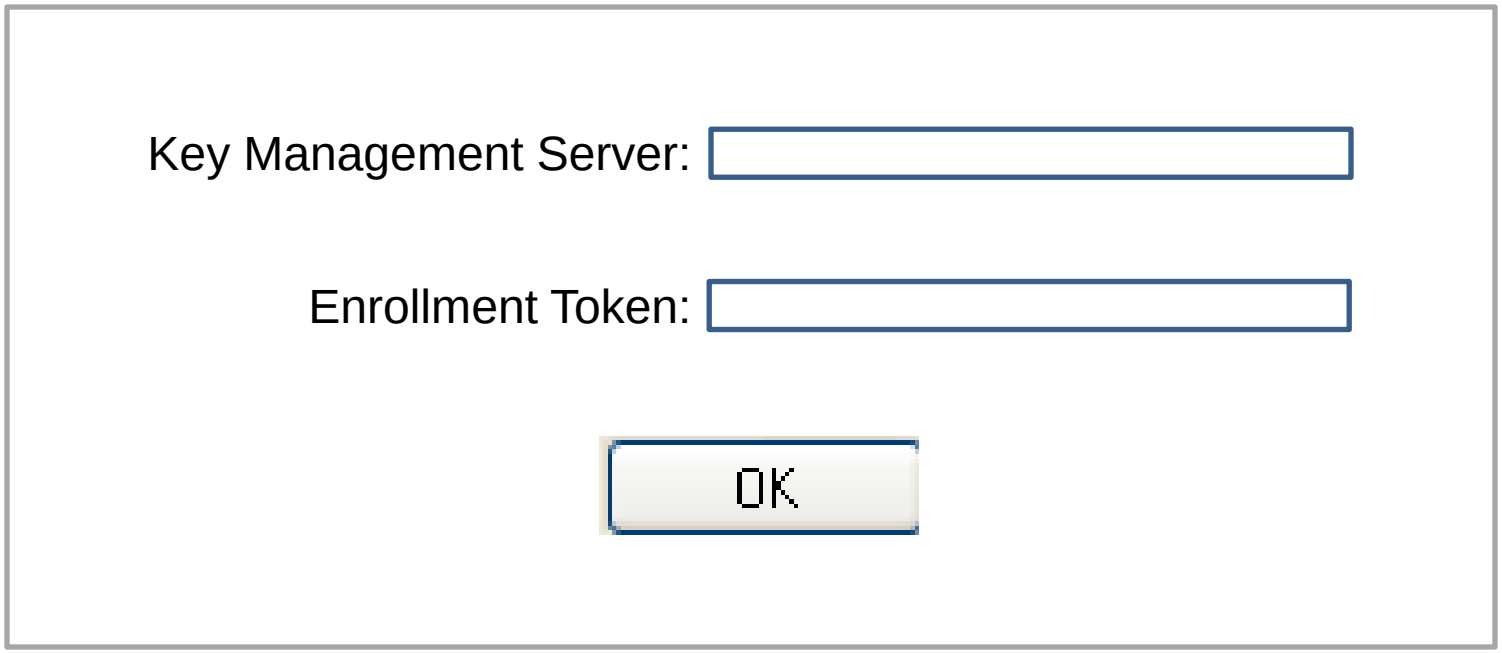


Full Process Flow: Security



Where we go from here

Client User Interface (suggested):



Where we go from here

- Removing decisions from clients
  - “How easy is this to screw up?”
  - Making Operational = Secure
- Key Management is first
- KM Metadata is second
  - Self-Describing Data (internal)
  - Metadata packaging (referential)

Summary

The enemy knows the system, and the allies do not.

Questions?

Jay Jacobs

jay.jacobs@target.com