PRACTICAL PKI

STEVEN BERNSTEIN

(@SCIATICNERD)

OVERVIEW & GOALS

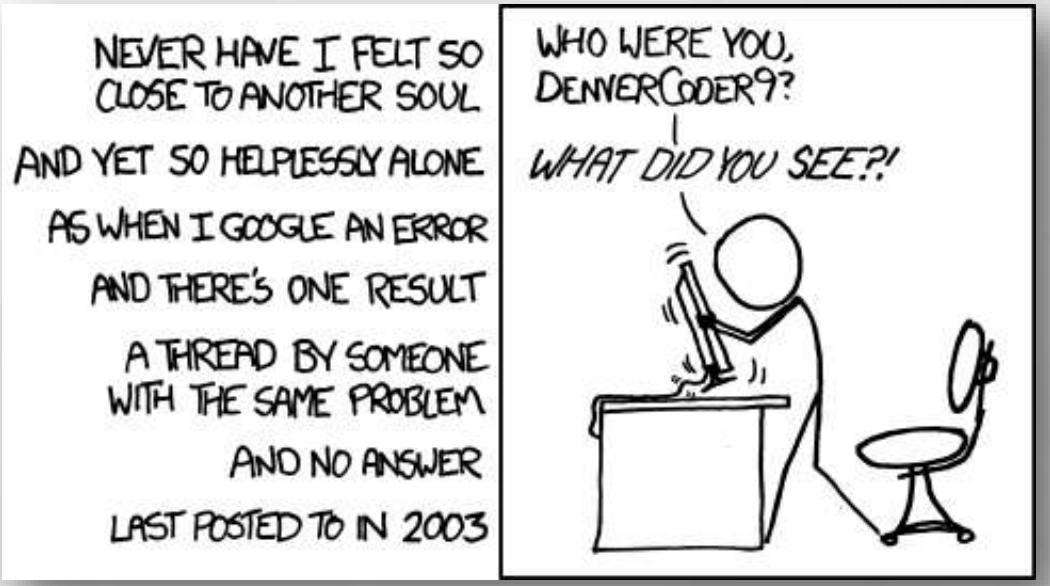
- IN THE BUILDING ≠ ACCESS TO THE PENTHOUSE
- CERTIFICATES ARE LIKE AUTOGRAPHS
- CHAINING AS A WHOLESALE CLUB
- VALIDATION BY NIGHT CLUB BOUNCER
- NOT JUST CLUBS, BUT STORES, TOO
- REQUESTING CERTIFICATES IS LIKE MAKING PIE
- GOVERNANCE & POLICY: STAY CLASSY
- CYBERSECURITY OS INTEL MOMENT

BUT... BUT... WHO ARE YOU?

- @SCIATICNERD
- 11 YEARS IN #INFOSEC
- ACTIVE SUPPORTER OF #BSIDES
- THAT KID WHO HUNG OUT IN THE A/V ROOM
- FRUSTRATED FILMMAKER
- SOMEWHERE BETWEEN KIRK AND CRANE (SHATNER & GRAMMER)

WHO IS THIS PRESENTATION FOR?

- TO HELP EXPLAIN TO PEOPLE OUTSIDE OF INDUSTRY
- NEEDED TO USE IT, BUT IT MADE NO SENSE
- ANYONE WHO WANTS TO LEARN
- NOT NECESSARILY CRYPTO FOLKS
- THE FRUSTRATED (SEE ATTACHED)



BUT WE KNOW PKI!

- GOAL IS TO GO OVER HOW THE PIECES WORK TOGETHER
- NO MATH REQUIRED
- KNOW YOUR CRYPTO?
  - AWESOME!
  - LEAVE MOST OF IT BY THE DOOR, PLEASE
- REMEMBER: THIS "CLASS" IS FOR NON-MAJORS

Apologies to Cory Doctorow
And those who made the example of double locked crypto using a tennis ball and padlocks

HOW CERTIFICATES ARE EXAMINED

Presentation	Examination	Chaining	Validation
CHECK ME OUT BRO	RIGHT NAME? NOT EXPIRED?	THIS FROM MY CLUB?	MEMBERSHIP CANCELLED?

"PKI BROKERED AUTHENTICATION" (SORTA)

IN THE BUILDING ≠ ACCESS TO PENTHOUSE

- AUTHENTICATION
  - IDENTITY (WHO YOU ARE IS NOT WHAT YOU DO)
  - PINS ARE A CHALLENGE FOR TOKEN HOLDERS
  - MACHINES ARE PEOPLE TOO?
- AUTHORIZATION
  - DESCRIBES WHAT AUTHENTICATED CREDENTIALS ARE ALLOWED TO DO
  - PROVISIONING ON THE FLY IS THE “HOLY GRAIL”

CERTIFICATES ARE LIKE AUTOGRAPHS

- WHO ARE YOU?
  - BOB AND ALICE AREN'T IN RIGHT NOW
  - MAY I HELP YOU, INSTEAD?
- OH HO HO, MAGIC!
- ELECTRONIC TRUST
- COLLECTION OF SERIAL NUMBERS AND RESULTS

CERTIFICATES ARE

- ELECTRONIC IDENTITY FOR PEOPLE AND TOYS
- HOW FAR DO WE TRUST IT?
- SOUNDS EASIER THAN IT IS, KINDA
- WHY CAN'T WE JUST USE SELF-SIGNED CERTIFICATES?

CHAINING IS A WHOLESALE CLUB

- EXAMINATION OF CARD AT DOOR REQUIRED
- BASIC CHECKS WITHOUT HELP (VALIDATION)
- KNOWS WHICH CLUB A CARD HOLDER BELONGS TO
- ROOT CHAINS ESTABLISH WHICH CLUB A CERTIFICATE BELONGS TO

LOSTCO NOSALE

Mr. Turing Exp. 03/15

Sham's CLUB

VALIDATION BY NIGHT CLUB BOUNCER

- IF THE BOUNCER FINDS A MATCHING ENTRY ON THEIR CLIPBOARD, IT'S TO PREVENT ACCESS
- A CERTIFICATE REVOCATION LIST REPLACES THE CLIPBOARD OF NAMES
- CALLED REVOCATION CHECKING OR CERTIFICATE VALIDATION

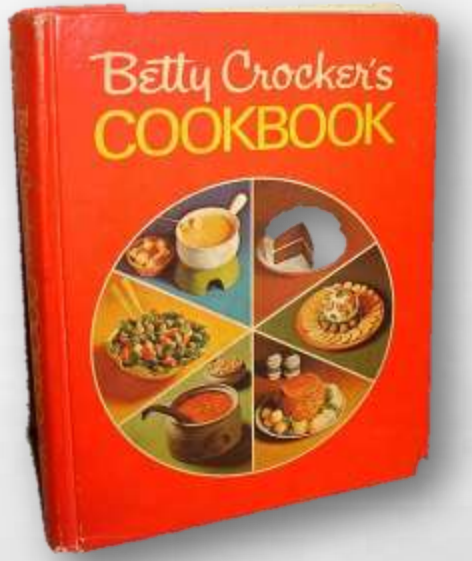
NOT JUST CLUBS, BUT STORES, TOO!

- WHY NOT JUST TRUST EVERYBODY?
- TUCKED IN MORE PLACES THAN A HOLLYWOOD HAS-BEEN
- HOW DO WE DECIDE WHO SHOULD STAY?
- MORE THAN ONE ON EVERY MACHINE
- GO ASK MOXIE – CAN'T TRUST 'EM ALL

Drive-thru Trust Decisions Will Leave You With Heart burn

REQUESTING CERTIFICATES IS LIKE MAKING PIE

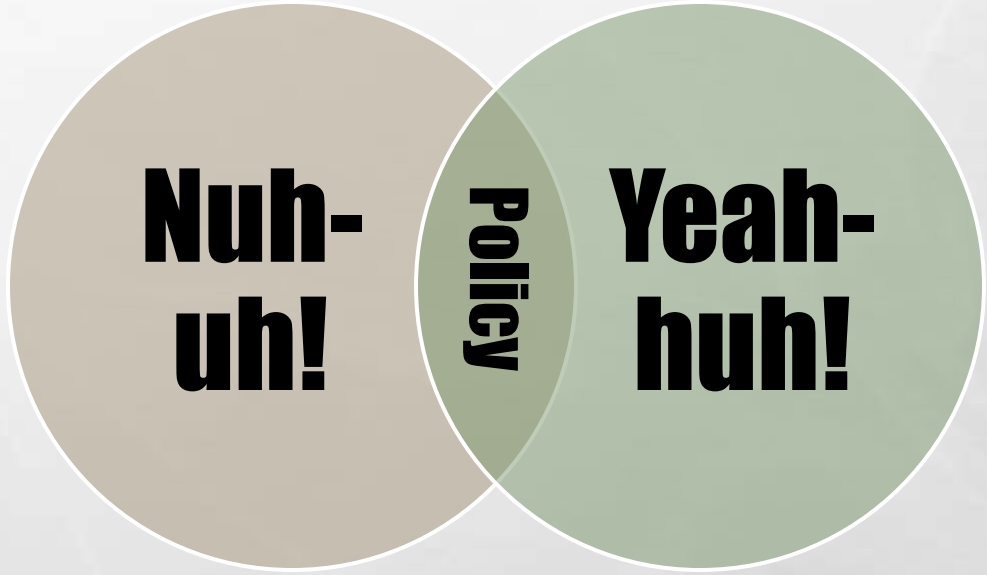
- ALWAYS STARTS WITH MAKING CRUST
  - BOILS DOWN TO GETTING A CERTIFICATE
  - DIFFERENT TOOLS MAKE IT MORE CONFUSING
- IT'S THE FILLING THAT CHANGES
  - KNOWING WHAT STEP YOU'RE ON HELPS
  - MARK THE EXPIRATION DATE ON A CALENDAR



Generate → Backup → Submit → Coordinate → Retrieve → Pair → Archive

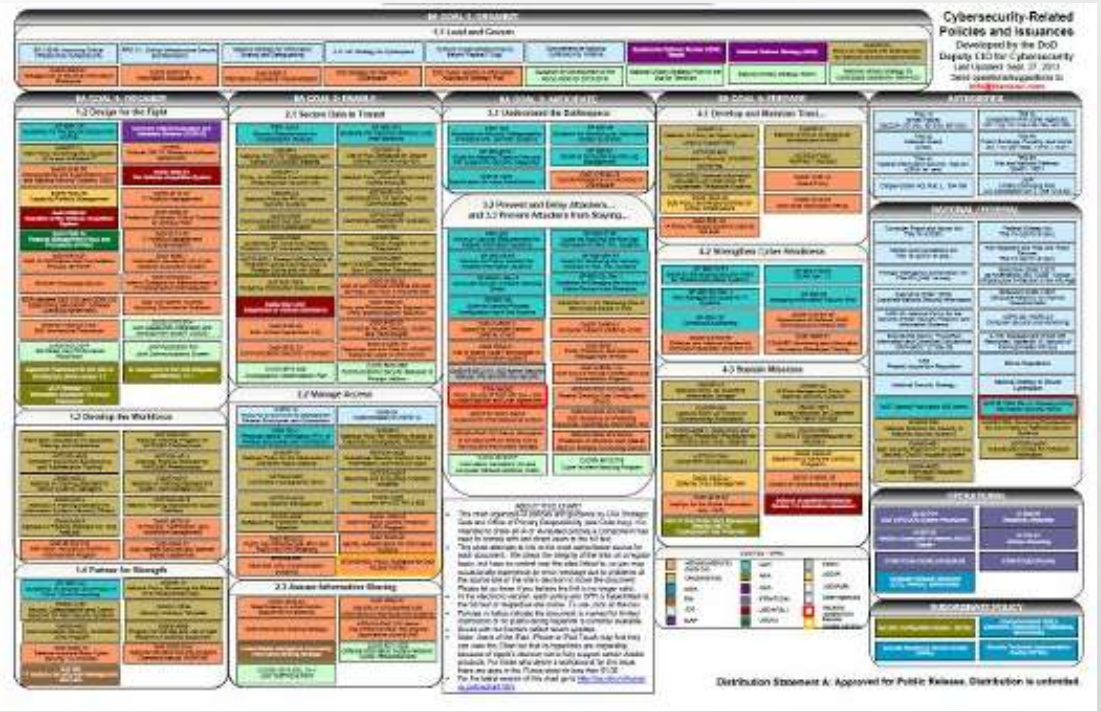
GOVERNANCE & POLICY: STAY CLASSY

- POLICY DISCUSSIONS ARE LIKE PLAYING A GAME OPERATION (TM) WITH A BUNCH OF 5 YEAR OLDS, ARGUING OVER THE RULES THAT ARE WRITTEN INSIDE THE BOX TOP.
- GOVERNANCE AND PKI
  - CERTIFICATE POLICY: THE RULES
  - CERTIFICATION PRACTICE STATEMENT: HOW TO APPLY THE RULES



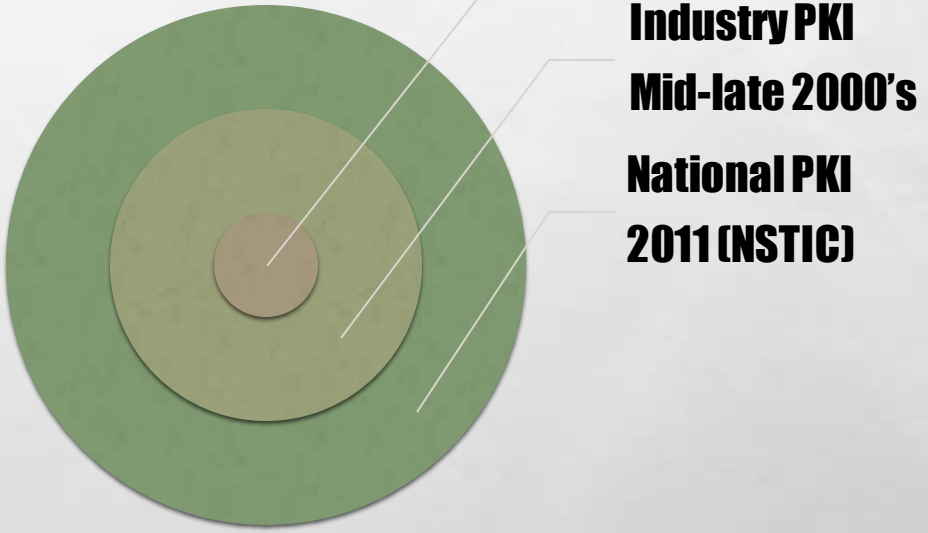
GOVERNANCE & POLICY: STAY CLASSY

- POLICY. NOT ALWAYS GLAMOROUS.
- IT HELPS IF YOU CAN HOLD A GRUDGE
- EXPLAINS ALL THE SCOTCH, NOW DOESN'T IT?
- SOMETIMES IT HELPS TO HAVE AN ART DEGREE
  - THE IMPORTANCE OF NEGATIVE SPACE
  - SHOULD BE WRITTEN TO STAND ON ITS OWN



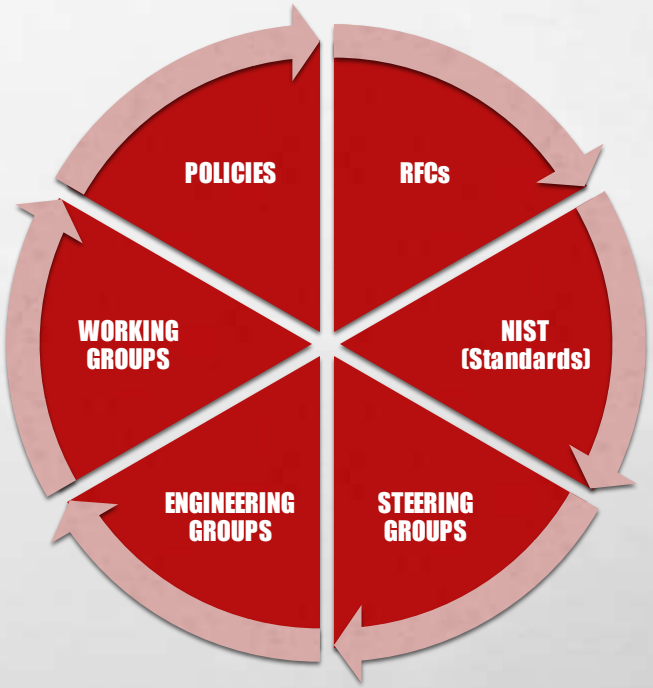
CYBERSECURITY OS INTEL MOMENT

- PKI ISN'T NEW: IN PRODUCTION SINCE 90'S
- RISE / RETURN OF THE SMART CARD IN U.S.
  - REMEMBER AMEX BLUE? EMV?
- ECA PKI ► INDUSTRY PKI ► NATIONAL PKI
- NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: IDMANAGEMENT.GOV
- PKI IS PLANNED FOR, NOT INSTANT ON



SECOND VERSE SAME AS THE FIRST

- POLICY DEVELOPMENT HAS A CYCLICAL FLOW
- OPPORTUNITY TO GET INVOLVED
- THIS COULD DOVETAIL WITH OTHER EFFORTS
- CONSIDER @IAMTHECAVALRY OR OTHERS
- SILENCE EQUATES WITH ASSENT HERE
- SEVERAL STAGES ALLOW FOR INTERACTION



REVIEW OF WHAT WAS COVERED

- IN THE BUILDING ≠ ACCESS TO THE PENTHOUSE
- CERTIFICATES ARE LIKE AUTOGRAPHS
- CHAINING AS A WHOLESALE CLUB (ROOT CHAINS)
- VALIDATION BY NIGHT CLUB BOUNCER
- NOT JUST CLUBS, BUT STORES, TOO
- REQUESTING CERTIFICATES IS LIKE MAKING PIE
- GOVERNANCE & POLICY: STAY CLASSY
- CYBERSECURITY OS INTEL MOMENT

SciaticNerd will return in:

ANY QUESTIONS ON PRACTICAL PKI?

STEVEN BERNSTEIN

(@SCIATICNERD)