Knock Knock, Who is There?

Dustin Hayes
Vanguard Integrity Professionals

How did we get here…

Top WHAT?

KNOWLEDGE IS THE BEST DEFENSE

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

VANGUARD SECURITY & COMPLIANCE

But I don't want to…

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	**Severe**	**Major**	**99%**
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	**Severe**	**Minor**	**73%**

But I don't want to…

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

But I don't want to…

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	**High**	**Moderate**	**82%**
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	**Medium**	**Moderate**	**75%**
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

But I don't want to…

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	**High**	**Minor**	**80%**
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

But I don't want to…

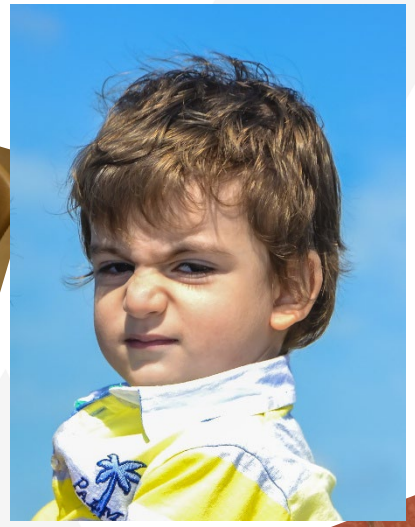
Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	**Medium**	**Moderate**	**79%**
User IDs with no Password Interval	**Severe**	**Major**	**75%**
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

Because it does not describe risk

Finding Description	Severity	Remediation	Occurrence
Network Communication not Secured using TLS	Severe	Major	99%
UNIX System Services Directories with World WRITE	High	Major	96%
UNIX System Services Files with World WRITE	High	Major	93%
Inappropriate UMASK Value Set	High	Moderate	87%
Excessive Access to the USER CATALOG Data Sets	High	Moderate	82%
Excessive Access to the SMF Dump Data Sets	High	Minor	80%
CICS APPLID is not Controlled by VTAMAPPL Profiles	Medium	Moderate	75%
Two Factor Authentication is not Required for Elevated Users	Medium	Moderate	79%
User IDs with no Password Interval	Severe	Major	75%
Excessive Access to the System REXX Data Sets	Severe	Minor	73%

INSTEAD LET US DISCUSS…

Who tends to give us a call…



- The Parent
- The Test Taker
- The Follower
- The Investigator
- The Responder

Anyone know who this person is?

Alfred Charles Hobbs

Born: October 7th 1812
Died: November 6th 1891

He was the first one to pick Bramah's lock and the Chubb detector lock at the Great Exhibition of 1851, and so forced lock manufacturers to improve their designs

"Rogues are very keen in their profession, and know already much more than we can teach them."

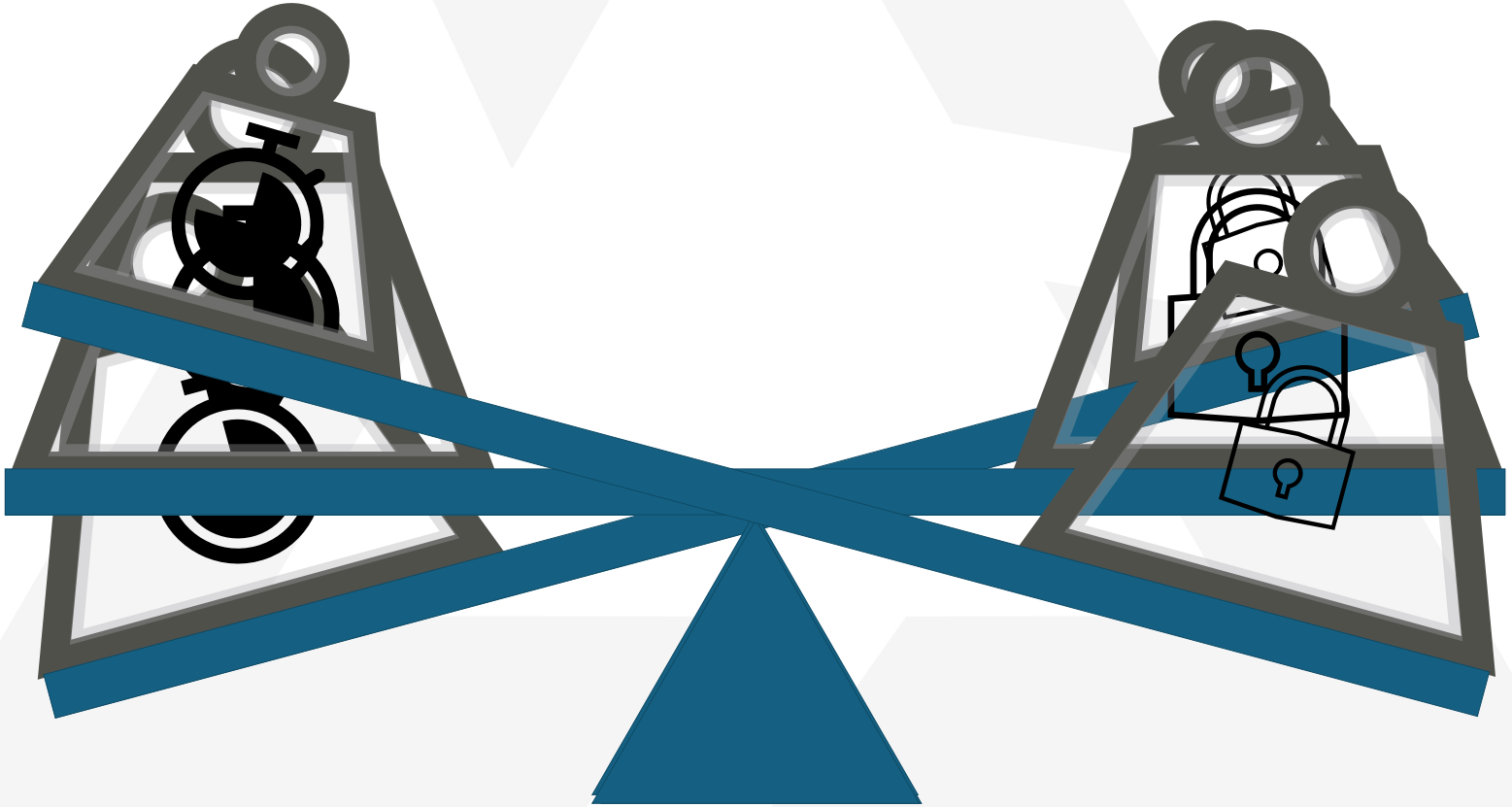
Alfred Charles Hobbs in 1853 when questioned on the wisdom of publishing the weaknesses of existing locks.

Source: Alfred Charles Hobbs - Wikipedia

What is my goal

Operations

Security



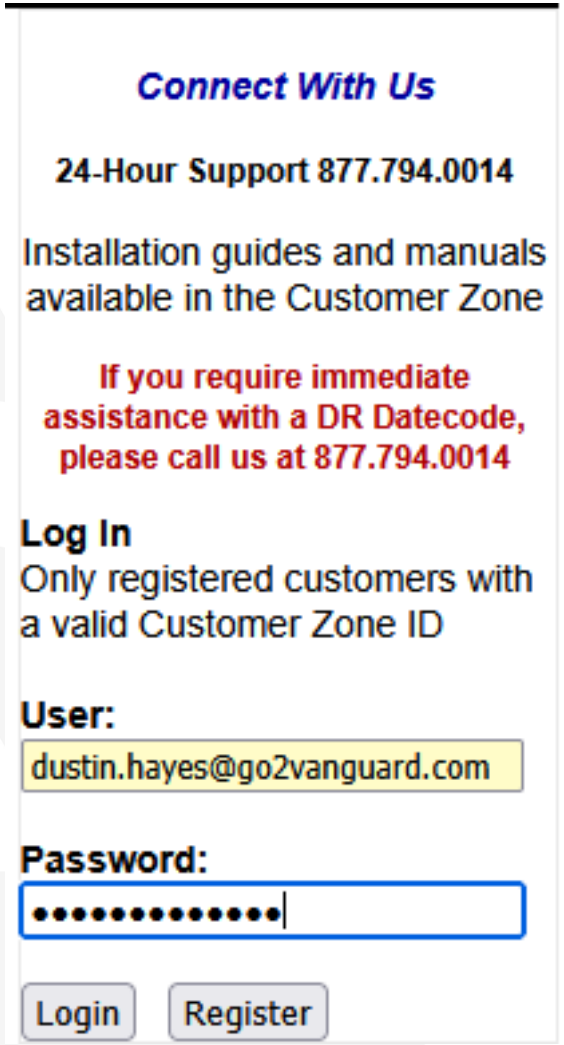
SOME THINGS I HAVE SEEN

Have we gone too far?

The logon page for Vanguard customer zone →

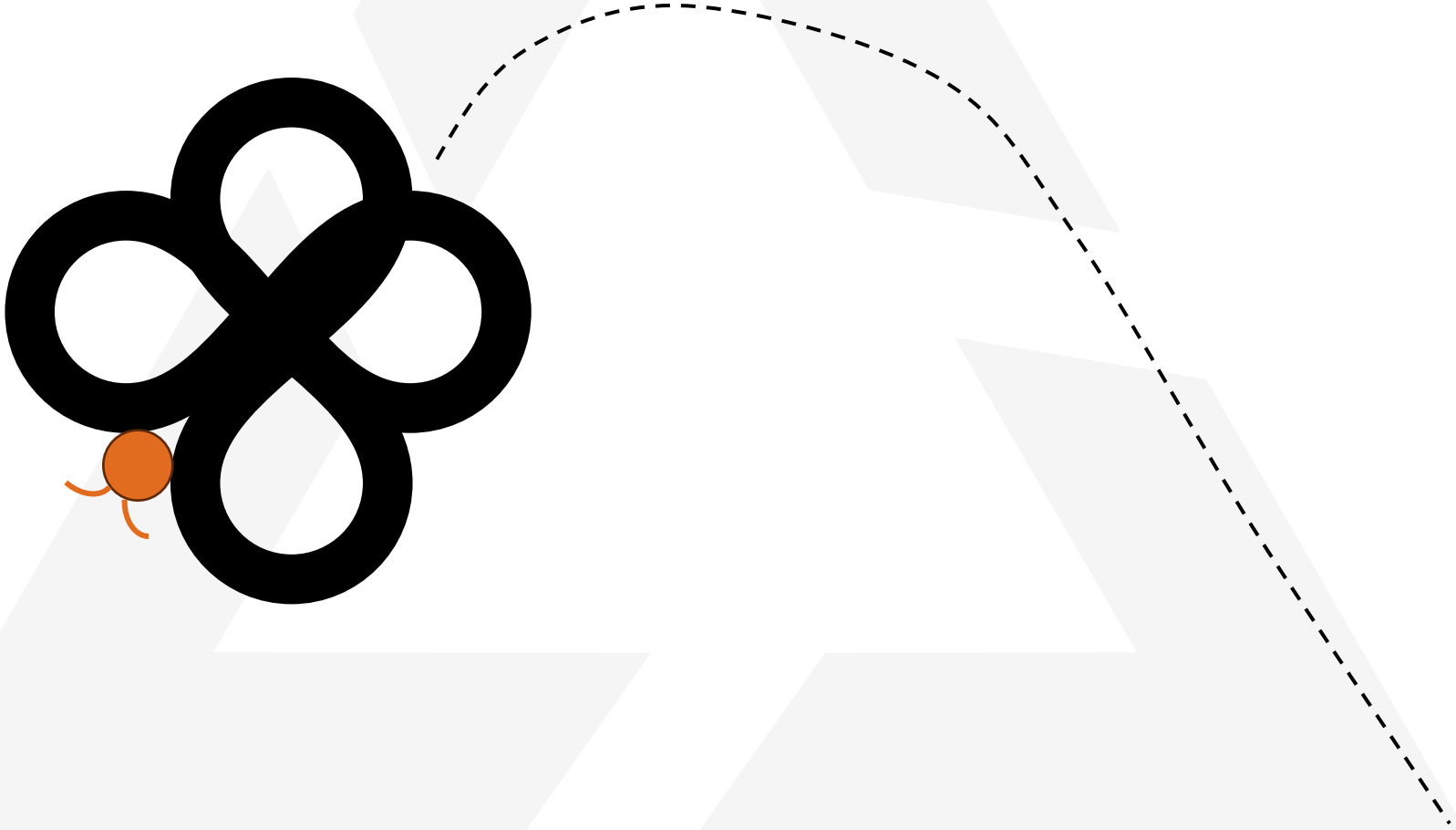
Recently a customer wanted us to update to:

- Minimum 15 Character Password
- Changed every 60 days
- 3rd Party Authenticate to their Azure w/ MFA
- Monthly report of all logins provided to them



Another example of going too far…

A story about a password…



I'm following the "New Password Rules"

NIST SP 800-63B-4 – Section 3.1.1.2 "Password Verifiers" summarized as

1. The length of the password
    1. Single Factor - *SHALL* have minimum of 15 characters in length
    2. Multiple Factors - S*HALL* be a minimum of 8
2. Password *SHOULD* have a maximum length of at least 64
3. Password *SHOULD accept all printed ASCII/Unicode characters and a space*
4. Password *SHALL NOT* impose other composition rules
5. Password *SHALL NOT* require periodic password changes
6. Password *SHALL NOT* permit the storage of a password hint
7. Password *SHALL NOT* prompt the use of knowledge-based authenticators
8. Password *SHALL* be supplied in full

EXPANDING BEYOND PASSWORDS

Providing by Default in RACF

Remember this?

Chapter 2. Using ISFPARMS for customization

This topic describes SDSF's internal parameters, ISFPARMS, and explains how to use ISFPARMS to customize SDSF.

Important: SDSF does not support security via the ISFPARMS mechanism. All users of SDSF 2.5 must use the Security Authorization Facility (SAF) with an External Security Manager (ESM) such as RACF, ACF2, or TSS. For information about migrating from using SDSF security with ISFPARMS (ISFPRMxx or ISFPARMS with assembler macros) to RACF security, refer to z/OS SDSF Security Migration Guide.

Note: SDSF provides a utility for converting ISFPARMS assembler macros to ISFPRM*xx* statements. See "Converting ISFPARMS assembler macros to statements" on page 6.

Source: IBM's z/OS SDSF Operations and Customization Version 2.5 **(SA23-2274-50)**

"Protected by Default"

Despite what we have all been told…

RACF

- What happens when RACF Returns RC=4

ACF2

- "Dustin your wrong, ACF2 is better than RACF it provides protection by default"

Top Secret

- "Dustin you will love TSS, it just makes sense"

Protected by Default (in ACF2)

Despite what we have all been told…

Unintended Consequences

- Sometimes we must enter a SAFDEF to for a RC=4

Clearly documented exceptions

- Broadcom's Processing SAF Calls section

Choices by "your company"

- Changes to a LID to bypass "protection by default"

Protected by Default (in TSS)

Despite what we have all been told…

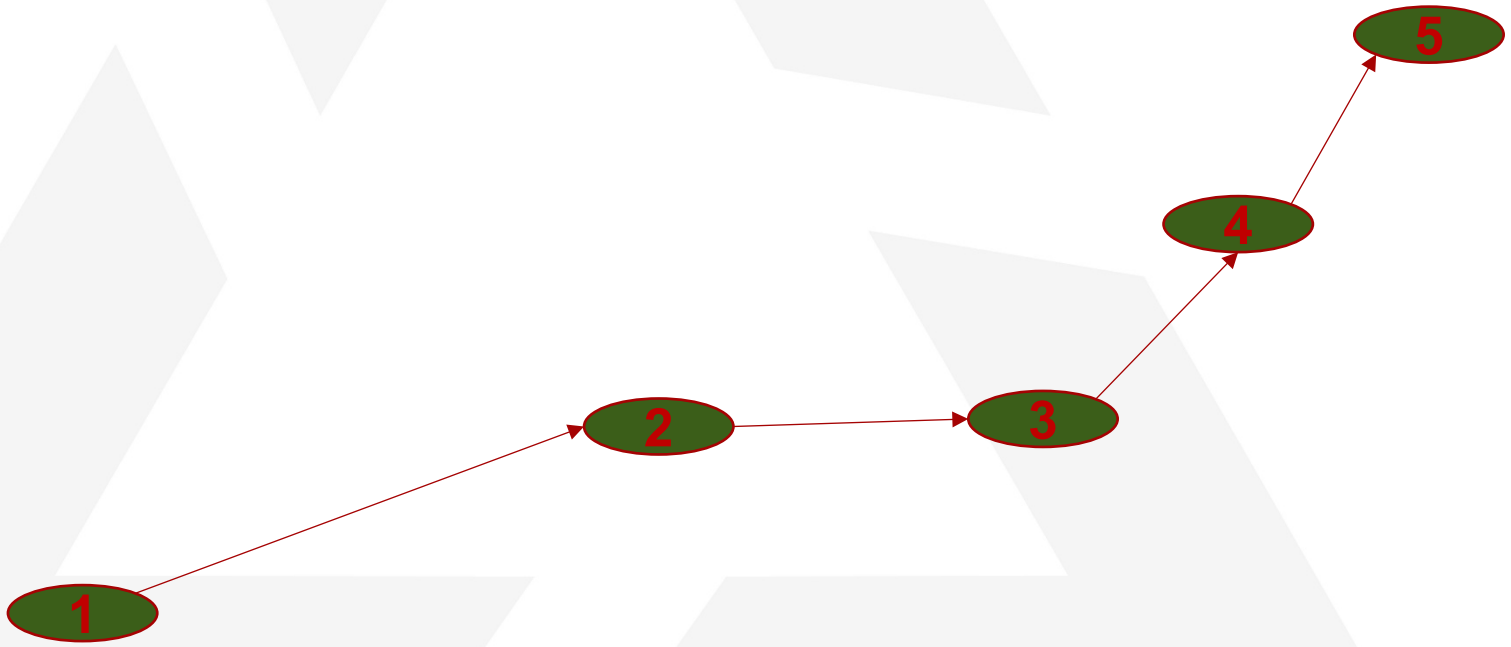
Choices by "your company"

- Changes to an ACID to bypass "protection by default"

The value of *<NULL>*

- A harder concept than - There are 10 types of people in this world: those who understand binary and those who do not

A Practical Example of a Penetration Test



SUGGESTIONS

A high-level approach

- Understand your risk and impact
  - Biggest way to stop common events?
- Obscurity verse Security
- Remember to listen for personalities
- Maybe Silly … but why?

Your feedback is important!

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation