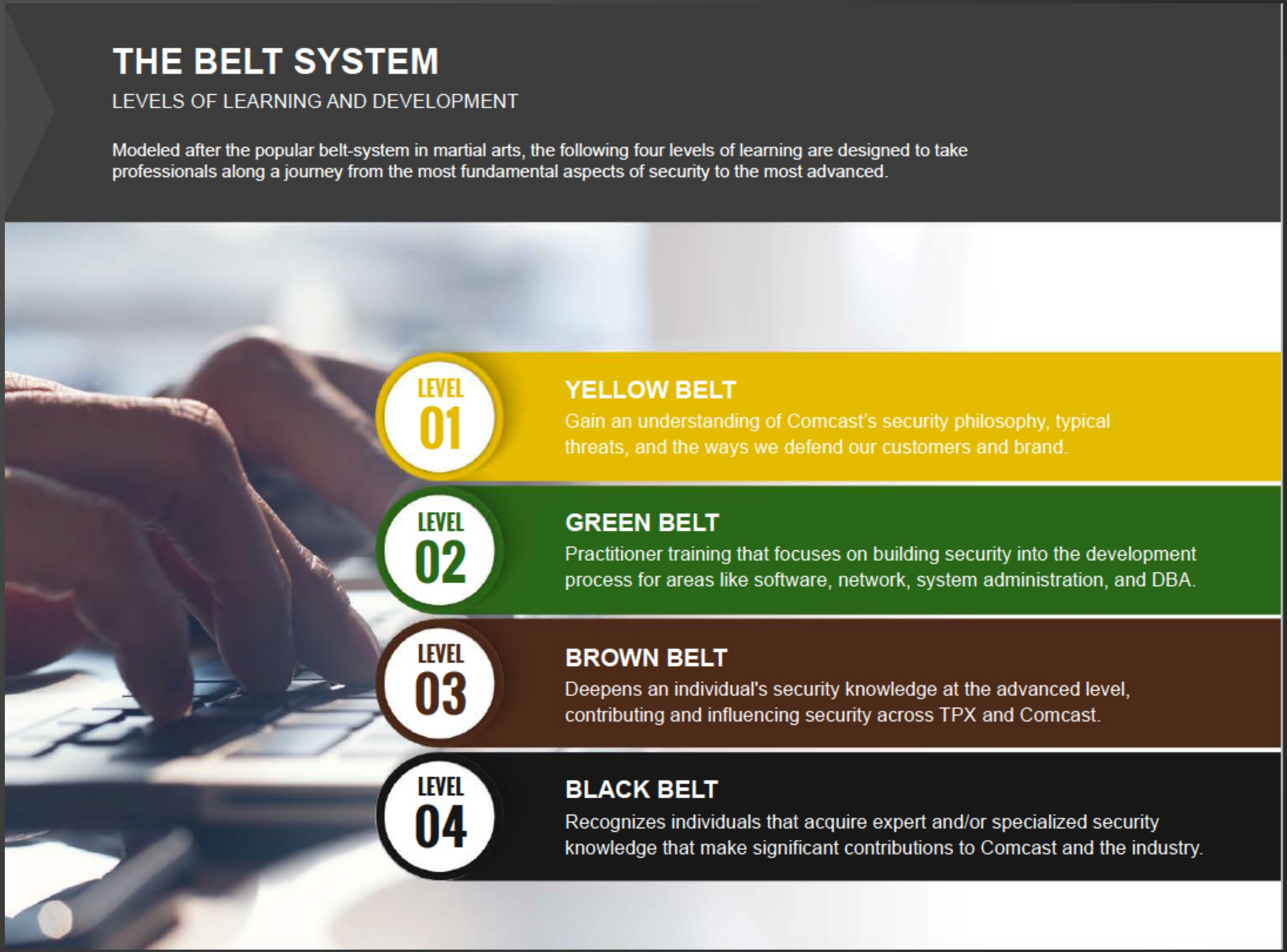
Secure Software Development Training at Comcast

About the Green Belt Security Training

and some of the material covered

TPX Security Learning Program



THE BELT SYSTEM

LEVELS OF LEARNING AND DEVELOPMENT

Modeled after the popular belt-system in martial arts, the following four levels of learning are designed to take professionals along a journey from the most fundamental aspects of security to the most advanced.

LEVEL 01

YELLOW BELT

Gain an understanding of Comcast's security philosophy, typical threats, and the ways we defend our customers and brand.

LEVEL 02

GREEN BELT

Practitioner training that focuses on building security into the development process for areas like software, network, system administration, and DBA.

LEVEL 03

BROWN BELT

Deepens an individual's security knowledge at the advanced level, contributing and influencing security across TPX and Comcast.

LEVEL 04

BLACK BELT

Recognizes individuals that acquire expert and/or specialized security knowledge that make significant contributions to Comcast and the industry.

What’s a Green Belt?

- A six month program for acquiring skills and knowledge on security topics
- Focuses on building security into the development process
- Structured following a Learn, Share and Do model

OK, but what did you study?

- Data privacy within Comcast
- Threat Modeling Overview
- Web Application Pen Testing Fundamentals
- Secure Coding Practices (Android)
- Cryptography overview
- Mobile Device Security
- HTTPS in depth
- Kali Linux and Ethical Hacking

CIA Triad of Infosec

- **Confidentiality** – only authorized individuals, entities or processes have access to the data.
- **Integrity** – the data must be accurate and complete.
- **Availability** - the data must be available when needed.

Cryptography: Art & Science

- The art of writing and solving codes (Google)
- The science of encipherment and decipherment in secret code or cipher (Merriam-Webster)

Cryptanalysis

- The art of breaking codes and ciphers

Caesar Cipher

Modern Examples

- SSL, TLS (HTTPS)
- VPN
- Hash
- Digital Signatures

Hashing Algorithms

~ data integrity ~

- A Hash algorithm is a one-way function that once data is run through it, produces a unique value that will be the same every time the same file is run through.
- SSL uses hash algorithms for digital signatures

Hashing Algorithms

~ collisions ~

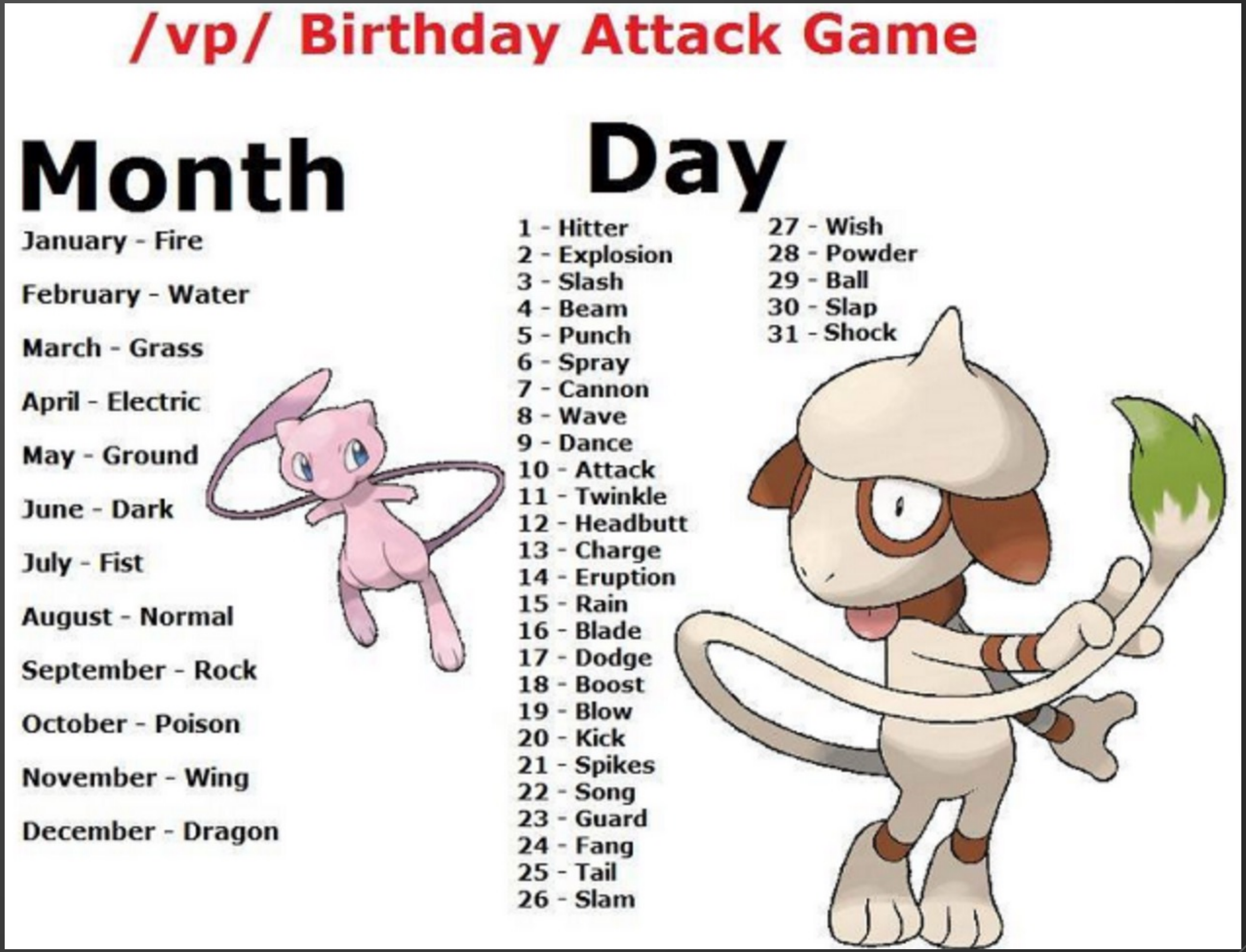
Hashing Algorithms

~ collisions ~

- Collisions are when the same hash can be produced by entering a different input.
- An attacker can create collisions to pass off malicious files or data as having a correct and proper hash
- MD2 and MD4 produce 128 bit value and are considered vulnerable to collision attacks since 1989 and 1990

Hashing Algorithms

~ birthday attack ~



/vp/ Birthday Attack Game

Month

January - Fire

February - Water

March - Grass

April - Electric

May - Ground

June - Dark

July - Fist

August - Normal

September - Rock

October - Poison

November - Wing

December - Dragon

Day

1 - Hitter
2 - Explosion
3 - Slash
4 - Beam
5 - Punch
6 - Spray
7 - Cannon
8 - Wave
9 - Dance
10 - Attack
11 - Twinkle
12 - Headbutt
13 - Charge
14 - Eruption
15 - Rain
16 - Blade
17 - Dodge
18 - Boost
19 - Blow
20 - Kick
21 - Spikes
22 - Song
23 - Guard
24 - Fang
25 - Tail
26 - Slam
27 - Wish
28 - Powder
29 - Ball
30 - Slap
31 - Shock

Hashing Algorithms

~ birthday attack ~

- MD5 incorporates an additional round of encryption than MD4 and outputs a fixed, 128 bit string for every input
- Because of the fixed output, MD5 is susceptible to birthday attack (1992) and is no longer used in SSL or digital signatures

Hashing Algorithms

~ SHA-256 ~

- **S**ecure **H**ash **A**lgorithms
- The SSL industry has picked SHA as its hashing algorithm for digital signatures
- Since 2016, SHA-2 has been considered the secure hash standard
- SHA-256 produces a 256 bit hash, with such a large number of possible combinations that the chance for collisions is minimal

The Keys

Symmetric Key

- Uses the same key to encrypt and decrypt (shared key)
- Strength comes from the key size and algorithm
- Difficult to crack when config has long enough keys
- Current uses: Credit card transactions

Symmetric Key

- DES – key size of 56 bits became vulnerable to brute force attacks as computational power increased
- Triple DES - uses a key bundle of 3 DES keys, but due to discovered vulnerabilities is considered a weak cipher
- AES – Support 128-, 192- and 256-bit encryption keys. Accepted as current standard for symmetric encryption

Asymmetric Key

- Uses a private and a public key
- The public key is made available to anyone who wants to send a message
- The sender encrypts using the public key
- The message can only be decrypted with the receiver’s private key

Asymmetric Key

- Strengths
  - Secure key exchange and simplified key management
  - Provides authentication as well as encryption
  - Supports digital signatures
- Weaknesses
  - Slower and less efficient than symmetric key algorithms

Asymmetric Key

- Popular asymmetric key encryption algorithms include
  - ElGamal
  - RSA
  - DSA
  - Elliptic curve techniques
  - PKCS

Asymmetric Key

- Diffie-Hellman Algorithm
  - Meant to address shortfalls of symmetric key encryption
  - Uses public and private keys to generate a symmetric key
  - Vulnerable to man-in-the middle attacks because it does not provide authentication when public keys are exchanged

Thank you!

- Thank you for letting me share some of what I learned during the Green Belt program. I hope you found the material informative and useful!