

Entrevista al equipo de Backend de Tuenti



Mucho se ha hablado en Security by Default sobre redes sociales (en mi caso, centrándome siempre en Tuenti) y siempre hemos tenido solamente una visión, la nuestra. Se me ocurrió hace unos meses que podía ser interesante organizar una entrevista con el equipo de Backend de Tuenti (evitando a departamentos de comunicación) y que nos contaran, desde la perspectiva de la seguridad, el funcionamiento interno de la red social. En un primer momento iba a ser una entrevista en video pero voy a estar unos meses 'fuera de combate' así que hemos optado por la opción clásica.

Antes de empezar, agradecer a Guillermo Pérez (@bisho), responsable de Backend y Seguridad, todas las facilidades que ha puesto para poder llevar a buen puerto la entrevista. Todos los que hayáis reportado alguna vez una vulnerabilidad habréis tratado con él, y a los que no, deciros que el trato recibido siempre ha sido ejemplar (y eso que no siempre hemos coincidido y hemos tenido algún que otro roce... :D). Agradezco también a Chema Alonso (@chemaalonso) por las preguntas que me propuso.

¡Comencemos!

La entrevista la he estructurado en cinco partes, seguridad del lado del equipo de desarrollo, del de la empresa, acerca del reporte de vulnerabilidades, seguridad/privacidad y finalmente un par de 'offtopic'.

1. Del lado del equipo de desarrollo

¿Qué metodología de desarrollo de código utilizáis?

Cada equipo tiene libertad para elegir su propio modelo de desarrollo, según las necesidades de cada área de producto. Casi todos los equipos de producto utilizan alguna metodología ágil, fomentándose mucho el test-driven development ([TDD](#)).

¿En qué partes del desarrollo entra en juego la auditoría de seguridad?

Desde el principio, por supuesto. Desde el mismo momento en que se está diseñando un servicio nuevo, se tiene en cuenta la seguridad y las reglas de privacidad. No sólo el código es revisado por otros miembros del equipo u otros equipos, sino que las especificaciones de producto y técnicas también pasan revisiones de otros equipos.

Por ejemplo para diseñar la plataforma de juegos, hicimos mucho hincapié en la privacidad, generando identificadores de usuario diferentes de los de la plataforma, distintos para cada proveedor de juegos, no proporcionamos la lista de amigos completa, sino sólo los amigos que hayan aceptado también las condiciones de privacidad del mismo juego, y un sin fin de medidas adicionales. Todo para proteger a los usuarios y limitar la información que se cede a terceros. Es un gran esfuerzo, requiere más computación y sube la barrera de entrada de nuevos proveedores de juegos, pero es un buen ejemplo del esfuerzo y el compromiso con la seguridad y la privacidad en Tuenti desde la misma fase de diseño de los productos.

¿Tenéis algún equipo de testing de código con tests unitarios, de regresión, fuzzing y demás técnicas?

Por supuesto. Tenemos un equipo de QA, release y testing frameworks (amplios y dedicados).

Tuenti tiene una amplísima batería de tests, desde unitarios hasta de aceptación con navegadores automatizados. Usamos [Jenkins](#) con múltiples instancias donde se prueban las ramas de desarrollo, que necesitan pasar todos los tests antes de ver la luz verde para 'mergear' el código al repositorio de integración. Este, a su vez, vuelve a pasar todos los tests en cada 'merge' antes de que salga a producción.

Aún siendo muy exhaustivos con los tests, el proceso está muy automatizado y resulta ágil. Somos capaces de hacer dos releases a la semana, con más de quince ramas de desarrollo en cada una, y nuestra intención es agilizarlo aún más.

¿Qué herramientas de tracking de bugs utilizáis internamente?

Actualmente estamos en una fase de transición de [Trac](#) a [Jira](#), ya que Trac se nos quedaba pequeño para el tamaño del equipo y el volumen de los datos. En otras áreas de la empresa como sistemas o soporte al usuario utilizan otras herramientas mejor adaptadas a sus necesidades.

Segun me comentasteis dais charlas internas los viernes... ¿Son realmente suficiente? ¿os habéis planteado que las imparta una empresa externa?

La formación es clave para una empresa como Tuenti. Las charlas técnicas de los viernes suelen ser de formación para nuevos empleados y las grabamos en vídeo para que estén siempre disponibles para cualquier recién llegado.

Normalmente las charlas son de miembros del equipo para explicar la filosofía de las herramientas, recomendaciones, etc., aunque no sustituyen al 100% a la documentación.

También se anuncian entre los empleados charlas que puedan resultar interesantes (sobre todo en Madrid y Barcelona que es donde tenemos oficinas), se fomenta la asistencia y se anima a participar como ponentes. Estamos abiertos a hospedar charlas técnicas externas en nuestras oficinas como las de [Madrid DevOps](#), [MadridJS](#) o [Python-Madrid](#), y patrocinamos numerosas conferencias.

Por último cada ingeniero tiene asignado un presupuesto que puede emplear para atender a conferencias técnicas. Hemos estado en el [Velocity](#) y muchas otras conferencias tanto nacionales como internacionales.

2. Del lado de la empresa

¿Habéis superado la ISO 27001?

En Tuenti estamos absolutamente concienciados sobre la seguridad y seguimos buenas prácticas alineadas con esta ISO, pero implantarla supondría una carga operativa importante en todos los procesos y por el momento no lo hemos hecho.

Empresas como Microsoft, Google, o Facebook, contratan auditorías whitebox/blackbox a empresas externas. ¿Ha auditado el código completo de la red social alguna empresa externa?

Grupos de Telefónica dedicados a la auditoría se encargan de las de tipo blackbox y estamos explotando sinergias para que se realicen auditorías de código pero, como el código de Tuenti es de una elevada complejidad y muy especializado, es difícil que herramientas automáticas den resultados aceptables (encargándose el equipo de QA de las pruebas manuales).

Uno de los principales problemas reportados por la Cloud Security Alliance es el del insider... ¿Hacéis auditorías de seguridad para saber quién ha accedido a qué perfiles de forma regular? ¿Tiene que reportarse todo acceso de un desarrollador o administrador a la base de datos de información en producción o backup?

Hemos pasado una auditoría de la AEPD muy recientemente. El equipo de ingeniería con acceso a datos es reducido y el acceso no es fácil. Los backups se encuentran aislados. Registramos la actividad de los equipos de soporte, que son más amplios, para controlar el mal uso de los permisos de administración, pero por el momento dichos registros son privados.

3. Reporte de vulnerabilidades

¿Cuántos reportes recibís y cual es su criticidad media? ¿Cuáles son los tiempos de actuación?

En el último trimestre tan sólo recibimos cuatro notificaciones de siete vulnerabilidades, y el anterior fue aún mejor.

Nuestro compromiso es solucionar las incidencias de seguridad en menos de 24h, aunque normalmente tardamos entre 1 y 2 horas.

La tendencia es claramente positiva, con cada vez menos incidencias (sobre todo en productos nuevos que antes eran un problema), siendo la criticidad de las mismas cada vez menor.

El fallo más habitual suele ser algún tipo de inyección XSS, que tienen una criticidad limitada ya que requieren que el atacante desarrolle una plataforma para el ataque.

Aunque no es una vulnerabilidad en sí misma, con diferencia, el mayor problema de seguridad es el phishing. Normalmente cada semana aparece alguna página nueva dedicada a engañar a los usuarios y robar credenciales. Bloqueamos la URL de inmediato y contactamos con los hostings y proveedores de DNS para cerrar la página lo antes posible. Tenemos contratada una empresa externa para el proceso, y actuamos por vía judicial si se averiguan datos de los implicados.

Ser rápidos es imprescindible para limitar la posible exposición de los usuarios y el beneficio obtenido por los atacantes. Cuanto menos sea el beneficio, menos interesante será Tuenti como plataforma a atacar, y por ello nos lo tomamos muy en serio.

También tratamos de concienciar al usuario, colaboramos con entidades públicas y privadas que trabajan en éste área explicando a los jóvenes cómo controlar su privacidad en Internet y disponemos de páginas de ayuda, pero el factor humano es siempre el eslabón más débil.

En el caso de que alguien encuentre una vulnerabilidad... ¿Cómo os la notifica? ¿Cómo gestionáis todos los reportes?

Atendemos todos los buzones de correo publicados en DNS además del estándar **security@tuenti.com**. No queremos publicarlo en la web para evitar que el volumen de correos no relacionados (realmente) con problemas de seguridad sea tal que los ingenieros tengan que dejar de atender la cuenta, y tener que ser filtrada por soporte al usuario. Actualmente tenemos un representante de cada equipo, y eso garantiza unos tiempos de respuesta bajísimos en comparación con muchas otras empresas del sector.

Las comunicaciones vía los canales de soporte al usuario también son filtrados y nos acaban llegando. Aunque el equipo de soporte es amplísimo y está muy formado, el proceso suele demorarse más tiempo hasta que llega a manos de los ingenieros.

En el caso de que se publiquen vulnerabilidades sin haber sido notificadas previamente, ¿cómo gestiona Tuenti la situación?

Lo primero nos centramos siempre en lo importante: tratar de solucionar el problema. Luego procuramos contactar con la persona que lo publicó para pedirle que la próxima vez nos lo notifique previamente, a fin de que ningún usuario se pueda ver afectado por un

fallo de seguridad. Les transmitimos nuestro objetivo de solucionar las incidencias en menos de 24 horas, y casi siempre la gente responde genial, se muestra muy dispuesta a colaborar y agradece nuestra actitud responsable y comprometida por la seguridad.

Recientemente enviastéis un C&D a un usuario por publicar una aplicación que monitorizaba el tráfico XMPP del chat de Tuenti (tema comentado aquí hace más de un año), ¿puedes comentarnos por qué llegastéis a tomar esa decisión si no era ninguna novedad?

Somos totalmente flexibles y tolerantes con la publicación de artículos, investigaciones e incluso segmentos de código, pero dar una herramienta ya lista es algo diferente, puede perjudicar a muchos usuarios. Actuamos igual que hacemos para casos de phishing y spam, una vez detectado, nuestro departamento legal envía un C&D estándar para tratar de mitigar el riesgo lo antes posible.

No obstante, a posteriori nos hemos puesto en contacto desde el área técnica con el autor para agradecerle su rápida colaboración y aclarar los motivos. Las relaciones han sido cordiales y estupendas, como entre todos los profesionales de este sector.

Hemos podido comprobar la buena acogida que ha tenido el 'Bounty Program' de Facebook... ¿Habéis pensado en algún tipo de reconocimiento para los que, desinteresadamente, os notifican vulnerabilidades?

Siempre he creído que una respuesta rápida y profesional es la mejor respuesta, y siempre procuramos agradecer las comunicaciones y mantener informado del estado a los investigadores. También tenemos previsto reconocer la labor en un "Hall of Fame" de seguridad. Por supuesto sólo aquellos que nos notifiquen las vulnerabilidades y nos permitan solucionar el fallo antes de la publicación serán susceptibles de ser incluidos en él. Por el momento no tenemos pensados bounty programs, aunque si que solemos mandar algún detalle, camisetas, el famoso bote de Conguitos...

4. Seguridad y Privacidad

¿Tenéis implementado algún motor antimalware para validar los enlaces que publican los usuarios en la red social contra bases de datos de, por ejemplo, Driven by URL malware?

Tenemos validadores de muchos acortadores, más de 125 actualmente, aunque obviamente no es posible estar siempre 100% al día. También tenemos sistemas anti spam y anti malware automáticos y podemos bloquear URLs concretas dentro de la plataforma.

Control de privacidad, ¿es suficiente?

Creemos que lo simple es al final lo más conveniente. Sistemas más complicados acaban haciendo complejas las implicaciones y causando más fallos que beneficios.

Tuenti es cerrada, intenta que los usuarios sólo acepten a sus verdaderas amistades y que la información sea siempre relevante.

Además, en el caso particular de juegos y aplicaciones de terceros, como he comentado antes, hemos puesto mucho énfasis en la privacidad y protección de nuestros usuarios. No sólo redujimos la información enviada de cada usuario (por ejemplo, nunca se facilita el

correo electrónico del usuario, al contrario que otras redes sociales) sino que los contratos que firman los proveedores de juegos están muy blindados a favor de la privacidad del usuario son muy estrictos con el manejo y almacenamiento de su información.

¿Qué ocurre con los datos cuando los borramos?

La ley nos obliga a guardar algunos datos de acceso durante un tiempo. Aparte de eso, los datos se borran físicamente de todos los soportes de almacenamiento. Las fotos también se borran, aunque este proceso, dado el elevadísimo volumen de datos que manejamos, tarda más.

Además, hay que comprender que el volumen de ficheros que se sirven en un sitio como Tuenti es tal que se suelen utilizar sistemas especializados, CDNs y servidores de estáticos. Éstos disponen de cachés que pueden tardar en actualizarse. Aún con todo, la diferencia es importante con respecto a otras redes sociales por nuestro marcado compromiso con la seguridad y la privacidad de los usuarios.

¿Se almacenan las conversaciones del chat?

No, nos las almacenamos. Sin embargo los usuarios nos lo están pidiendo y estamos trabajando en poder atender esta demanda cumpliendo con todos nuestros protocolos de privacidad.

Con respecto al manejo de sesiones... ¿tenéis pensado evitar que los identificadores de sesión sean comunes entre API y Web? ¿qué pasó con el firmado de peticiones?

Estamos trabajando para quitar la compartición de sesiones entre plataformas, pero surgen muchos efectos colaterales. Creo que pronto lograremos que al menos el session id de la web normal no sirva para la API, aunque tiene el inconveniente de que extensiones de navegador puede acabar pidiendo el login y contraseña a los usuarios, lo cual es una mala práctica.

El firmado de peticiones causaba muchos problemas con algunos navegadores, y actualmente estamos apostando por SSL en vez de soluciones complejas.

Pregunta obligada, ¿váis a implementar SSL tanto en la página como en el chat y la API?

Nuestra infraestructura ha avanzado bastante en estos meses con conexiones persistentes, persistencia de sesiones SSL y un nuevo sistema de balanceado, así que tenemos planificado ofrecer SSL pronto.

En cualquier caso, me gustaría reiterar que el principal problema de seguridad de las grandes plataformas en Internet es el phishing, muy por encima del robo de sesiones por interceptación de comunicaciones. Interceptar tráfico es más complicado, el target de usuarios es más reducido y el atacante queda más expuesto (tiene que estar en la misma red) que en un phishing donde se puede aprovechar el anonimato de Internet. Por no hablar de que las sanciones por violar la privacidad de las comunicaciones son muchísimo más severas.

Respecto a la implantación de SSL, no puedo dar fechas al respecto todavía, ya que en una plataforma tan grande como Tuenti siempre hay mucha casuística que resolver. Pero será más pronto que tarde.

5. Otras preguntas

Comentan os un poco el tema de las becas en Tuenti

Colaboramos activamente con las universidades y ofrecemos cursar proyectos de fin de carrera. Tenemos un catálogo de temas e ideas pero también estamos abiertos a sugerencias. Recomendando contactar con hr@tuenti.com a todo aquél interesado.

Además, hace poco organizamos el primer Hack/Programming Contest de Tuenti con muy buenos resultados, tanto por el feedback que nos dieron los participantes como por haber acabado haciendo ofertas a casi todos los finalistas. Aprendimos mucho de esta experiencia y esperamos mejorar los sucesivos contests que hagamos.

¿No crees que dar acceso a las betas privadas a las personas que os notifican vulnerabilidades sería una buena forma de fidelizar su colaboración?

Tenemos un sistema de lanzamiento de productos muy flexible que nos permite seleccionar a gente por diversos criterios, incluso selección manual de usuarios específicos. Actualmente estamos incluyendo a algunos colaboradores en los programas de beta, aunque depende mucho del producto, del secretismo necesario, de si se desea hacer pruebas de A/B testing sin polucionar, etc. Si algún investigador de seguridad desea ser incluido puede contactar con nosotros y lo evaluaremos.